2010-09

Use case analysis for adopting cloud computing in Army test and evaluation

Bolin, Jason S.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

USE CASE ANALYSIS FOR ADOPTING CLOUD COMPUTING IN ARMY TEST AND EVALUATION

by

Jason Scott Bolin

September 2010

Thesis Co-Advisors: Man-Tak Shing
James Michael

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Use Case Analysis for Adopting Cloud Computing in Army Test and Evaluation		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Jason Scott Bolin			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Cloud computing in theory can reduce the total IT lifecycle cost for the US Department of Defense by enabling the enterprise to provision shared software-, platform-, and infrastructure-level services in an on-demand pay-as-you-go fashion. One of the hurdles faced by the Department of Defense is that of developing an enterprise-wide strategy and policy for migrating the enterprise's data and applications to the cloud. This thesis supports the formulation of such a strategy and the accompanying policy by providing a concrete example of how the standard workflow processes used across the US Army test and evaluation programs can be modified to take advantage of cloud computing. The thesis presents a Use Case analysis of the existing collaboration and communication that takes place in these processes, focusing on three specific workflow processes—program management, report collaboration, and de-confliction of contention for test and evaluation resources— that could be improved upon through the use of cloud-based collaboration and communication services. Our results indicate that the cloud-based collaboration and communication services are much better suited to distributed large-scale planning, execution, and reporting of program test and evaluation than those used in the existing test and evaluation workflow processes. The thesis also provides recommendations on migration to cloud computing, how some of the results from this thesis are applicable to the entire Department of Defense enterprise, and suggestions for follow-on research.

14. SUBJECT TERMS Cloud Computing, Army Test and Evaluation (T&E) Command (ATEC), Data Center Consolidation, Area Processing Center (APC), Use Case Analysis, Program Management, Test Report, Document Collaboration, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)			**15. NUMBER OF PAGES** 149 **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

USE CASE ANALYSIS FOR ADOPTING CLOUD COMPUTING IN ARMY TEST AND EVALUATION

Jason S. Bolin
Civilian, United States Army
B.S., Tennessee Technological University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SOFTWARE ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2010

Author: Jason S. Bolin

Approved by: Professor Man-Tak Shing
Thesis Co-Advisor

Professor James B. Michael
Thesis Co-Advisor

Professor Peter J. Denning
Chairman, Department of Software Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cloud computing in theory can reduce the total IT lifecycle cost for the US Department of Defense by enabling the enterprise to provision shared software-, platform-, and infrastructure-level services in an on-demand pay-as-you-go fashion. One of the hurdles faced by the Department of Defense is that of developing an enterprise-wide strategy and policy for migrating the enterprise's data and applications to the cloud. This thesis supports the formulation of such a strategy and the accompanying policy by providing a concrete example of how the standard workflow processes used across the US Army test and evaluation programs can be modified to take advantage of cloud computing. The thesis presents a Use Case analysis of the existing collaboration and communication that takes place in these processes, focusing on three specific workflow processes—program management, report collaboration, and de-confliction of contention for test and evaluation resources—that could be improved upon through the use of cloud-based collaboration and communication services. Our results indicate that the cloud-based collaboration and communication services are much better suited to distributed large-scale planning, execution, and reporting of program test and evaluation than those used in the existing test and evaluation workflow processes. The thesis also provides recommendations on migration to cloud computing, how some of the results from this thesis are applicable to the entire Department of Defense enterprise, and suggestions for follow-on research.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADSS – ATEC Decision Support System

AEC – United States Army Evaluation Command

APC – Area Processing Center

APC2 – Army Private Cloud Computing

API – Application Program Interface

ARISS – Army Recruiting Information Support System

AST – United States Army Test and Evaluation Command Systems Team

AT&L – Acquisition, Technology, and Logistics

ATEC – United States Army Test and Evaluation Command

BMDS – Ballistic Missile Defense System

C&A – Certification and Accreditation

CIO – Chief Information Officer

COCOM – Combatant Commands

CPU – Central Processing Unit

CSA – Cloud Security Alliance

DaaS – Database as a Service

DARPA – Defense Advanced Research Projects Agency

DISA – Defense Information Systems Agency

DoD – United States Department of Defense

DoE – United States Department of Energy

DoI – United States Department of Interior

DOT&E – Director Operational Test and Evaluation

DREN – Defense Research and Engineering Network

DT – Developmental Test

DTC – United States Army Developmental Command

DT&E – Developmental Test and Evaluation

DTIC – Defense Technical Information Center

EC2 – Elastic Compute Cloud

FAA – Federal Aviation Authority

FedRAMP – Federal Risk and Authorization Management Program

FIPS – Federal Information Processing Standards

FISMA – Federal Information Security Management Act

GSA – General Services Administration

HQ – Headquarters

IaaS – Infrastructure as a Service

IO – Input Output

IP – Internet Protocol

ISP – Instrumentation Support Personnel

IT – Information Technology

JCS – Joint Chiefs of Staff

JRE – Java Runtime Environment

JVM – Java Virtual Machine

LAN – Local Area Network

LBL – Lawrence Berkeley National Labs

LFT&E – Life Fire Test and Evaluation

LRIP – Low-Rate Initial Production

MILDEPS – Military Departments

M&S – Modeling and Simulation

NASA – National Aeronautics and Space Administration

NBC – National Business Cloud

NEC – Network Enterprise Center

NIPRNet – Non-secure Internet Protocol Routed Network

NIST – National Institute of Standards and Technology

NOTAM – Notice to Airmen

NPS – Naval Postgraduate School

OMB – Office of Management and Budget

OS – Operating System

OSD – Office of Secretary of Defense

OT – Operational Test

OTC – United States Army Operational Test Command

PaaS – Platform as a Service

PDA – Personal Digital Assistant

PM – Program Manager

PMES – Performance Measurement Enterprise System

POC – Point of Contact

PSDT – Personnel Services Delivery Transformation

RACE – Rapid Access Computing Environment

RBAC – Role Based Access Control

R&D – Research and Development

RFP – Request for Proposal

RFTS – Request for Test Services

RM – Resource Manager

ROI – Return on investment

RSA – Redstone Arsenal

RSS – Rich Site Summary

RTC – Redstone Test Center

RTO – Responsible Test Organization

SaaS – Software as a Service

SDO – Standards Development Organization

SDREN – Secure Defense Research and Engineering Network

SER – System Evaluation Report

SIPRNet – Secure Internet Protocol Routed Network

SLA – Service Level Agreement

SOFIMS – SOMARDS Financial Information Management System

SOMARDS – Standard Operating and Maintenance Army R&D System

SDZ – Surface Danger Zone

TC – Test Center

TD – Test Director

TDY – Temporary Duty

TE – Test Engineer

T&E – Test and Evaluation

TM – Test Manager

TO – Test Organization

TSPI – Time Space and Position Information

QoS – Quality of Service

USD – Under Secretary of Defense

VDLS – Versatile Information Integration On-Line Digital Library System

VISION – Versatile Information Integration On-Line

VM – Virtual Machine

VOIP – Voice Over IP

WAN – Wide Area Network

WLAN – Wireless Local Area Network

ACKNOWLEDGMENTS

I would like to express special thanks to my amazing wife, Mary, who supported me during every step of my graduate studies. Her encouragement, support, motivation, and care of our son kept me focused during the many early mornings, late nights, and weekends this research required. I cannot express how blessed I am to have such a loving and understanding wife.

I would like to thank my advisors, Professor Shing and Professor Michael, for giving me a chance in 2006 when others would not, helping me scope this thesis, providing constructive feedback throughout the final review and for the patient guidance provided throughout my entire graduate studies. Through the course of this research I have come to realize how lucky I am to have had each as a teacher and advisor.

I would like to thank my current supervisor, Paul Jenkins, for the multiple sanity checks and reviews of my interpretation and depiction of the current ATEC Enterprise processes and procedures. Also for providing me with support at work by allowing me to attend conferences and informational meetings in my quest for knowledge about cloud computing.

Finally I would like to thank my former supervisor and mentor, David Browning, for first pushing me to begin my graduate studies and then supporting me throughout all of my endeavors within school and my career.

.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION

Within industry, it is estimated that roughly 66% of a business's information technology (IT) budget is spent on ongoing operations and maintenance and not on new initiatives and projects ("Enterprise and SMB Software Survey North America and Europe," 2008). If DoD's IT operating budget follows this trend, then roughly $20B (Lynn III, 2009) of DoD's 2010 IT budget, or 3.7% of DoD's total 2010 base budget ("Defense Budget 2010," 2010), could be spent on maintaining the status quo. To continue to support the warfighter and be fiscally responsible, DoD needs to eliminate the procurement and maintenance of redundant infrastructure.

Currently, DoD acquires hardware, software, and personnel that in essence perform the same function. The waste does not stop there. DoD must also pay for the hardware and software maintenance, licensing, facilities requirements (e.g., power, cooling, network, floor space), and keep personnel on staff to maintain everything. In September 2009, Deputy Secretary of Defense William Lynn III stated that within DoD there are approximately 15,000 networks comprised of 7 million computers, laptops, servers, and other devices. It takes an astounding 90,000 personnel to administer, monitor and defend those networks (Lynn III, 2009).

In June 2009, a memo was sent from the Executive Office of the President to the heads of departments and agencies regarding fiscal 2011 budget planning. What is interesting about this memo is that under information technology, cloud computing is specifically called out as a Presidential priority for IT. Specifically, the memo states that budget IT submissions "…should support the President's priorities for information technology, including transparency, participation and collaboration, and improving innovation, efficiency and effectiveness, in areas like cloud computing…" (Orszag, 2009) Within the President's 2011 budget, cloud computing is highlighted as a major part of the strategy to achieve efficient and effective IT. The Office of Management and Budget

(OMB), as part of the FY 2011 budget process, has requested all agencies evaluate cloud computing alternatives as part of their budget submissions for all relevant major IT investments. In FY 2012, agencies will be expected to tell OMB why they cannot use cloud computing for any new major technology project. In FY 2013, agencies must give OMB a complete alternative analysis for how existing projects could be moved to cloud computing.

Specifically:

- By September 2011 – all newly planned or performing major IT investments acquisitions must complete an alternatives analysis that includes a cloud computing based alternative as part of their budget submissions
- By September 2012 – all IT investment making enhancements to an existing investment must complete an alternatives analysis that includes a cloud computing based alternative as part of their budget submissions. This includes any project where funding is used for development, modernization, enhancement, or simply operations and maintenance (Miller, 2009)
- By September 2013 – all IT investments in steady-state must complete an alternatives analysis that includes a cloud computing based alternative as part of their budget submissions (Kundra, 2010)

While cloud computing is not a mandate, when the President asks you to consider something people tend to listen. Cloud computing holds promise to reduce IT infrastructure needs—both up-front and support costs, decrease maintenance/upgrades, improve resource utilization and collaboration capabilities. Although cloud-computing products are available these products are not mature enough to deliver the quality-of-service required by DoD.

In this thesis, we identify the requirements for cloud computing to support DoD's unclassified NIPRNet computing needs with a specific focus on workflow processes within the Army Test and Evaluation (T&E) domain. The U.S. Army was chosen because

it is the largest branch of DoD ("Bureau of Labor Statistics: Career Guide to Industries," 2010) and because the Army is pushing forward with plans to deploy an Army private cloud computing (APC2) environment. The request for proposal (RFP) for APC2 was released in late July 2010 with the stated goal of reducing cost and energy use while improving the Army's cyber-security posture and speed of innovation (Army Contracting Command, 2010). The APC2 is intended to be the cornerstone of a broader data center consolidation initiative that aims to reduce and consolidate the number of Army data centers to less than twenty (Hoover, 2010b).

In its present form, the Army has Network Enterprise Centers (NEC) located at 447 locations in the United States supporting nineteen different commands and agencies. The Army CIO has made it a top priority to realign and consolidate these NECs into two Network Service Centers (NSC) located in the United States and three abroad. At the heart of each NSC will be an Area Processing Center (APC), or consolidated data center (Sean Gallagher, 2010). APCs provide theater-level IT capabilities where functional and common-services information is stored, replicated, and centrally managed. The goal of an APC is to pull all applications and data storage out of local data centers at Army facilities and centralize it at a regional data center with applications mirrored across each APC. Data center consolidation is about determining how to collapse and provide more shared services, which also is a key step in adoption of the cloud (Link, 2010).

With APC2, the Army will be converting designated APCs into cloud computing environments that can provide shared services. The latest round of APCs being established includes Redstone Arsenal (RSA), Fort Knox, and Fort Bragg (Corrin, 2010). Since an Army T&E Command (ATEC) Developmental Test Center (DTC) subordinate command, Redstone Test Center (RTC), is located on RSA this research will approach the subject of a private DoD cloud from an Army T&E perspective. We assume that being collocated with an APC (i.e., utilizing the same fiber backbone) will provide the lowest possible latencies available in a cloud environment and as such would provide a best-case scenario for testing workflow processes.

B. RESEARCH QUESTIONS

This research attempts to answer the following questions:

1) What communications/collaborations do users use their computers for in the execution of a typical Army T&E program?
2) Can these interactions be abstractly modeled?
3) How would these collaborations/communications be carried out in a cloud based environment?

C. BENEFITS OF STUDY

This research will assist DoD in defining a roadmap for addressing the Presidential IT priority. This will be accomplished by:

- Providing a general overview of the current state of cloud computing
- Identifying issues that should be addressed before attempting to move to a cloud computing environment
- Analysis of the feasibility of a cloud environment in meeting the Army T&E mission through multiple use cases

D. ORGANIZATION

Subsequent chapters will focus on cloud computing concepts, as-is use cases, the study's results, and final conclusions.

Below are synopses of each chapter's contents:

1. Chapter II: Background

In order to have a firm foundation for the topics discussed, and a common lexicon, Chapter II provides a broad overview on cloud computing. The historical background leading up to the current cloud computing hype will be discussed. A brief definition and description of the core concepts of cloud computing will be covered and a brief overview of current efforts within the federal government will be given. The

overview of cloud computing will include discussions on: essential characteristics, architectures, deployment models, underlying value, and the identification of concerns that should be evaluated before moving to a cloud environment.

2. Chapter III: Current T&E Process

Chapter III presents several as-is use cases describing processes that could potentially be improved within a cloud environment. The scope for this chapter will be limited to the DoD Army T&E enterprise domain. The T&E domain will be used as an example to contrast the current as-is solution, as described in Chapter III, with a potential solution provided by a private DoD cloud, as described in Chapter IV. This chapter will provide a brief description of select systems within the Army T&E Enterprise Architecture. Use cases will be generated and a common high-level mission scenario will be used to walk through the current project management, range-test scheduling, and test-reporting process within ATEC. The selected use cases were chosen as they can readily be extrapolated to other domains within DoD. Every DoD activity also has project management, report collaboration, and asset utilization/scheduling concerns. Use cases, process diagrams, and collaboration diagrams are used in this thesis to model ATEC's T&E workflow processes.

3. Chapter IV: Cloud Based T&E Process

Chapter IV documents how a subset of the process, described within Chapter III, could be modified to leverage cloud computing. This chapter provides an assessment of how the mission scenario previously presented could be accomplished within a private DoD cloud. A subset of the use cases, process, and collaboration diagrams from Chapter III will be assessed to see how cloud computing, in its current form, could potentially streamline existing processes while also providing additional functionality, visibility, and reducing latency in delivering information to senior leadership.

4. Chapter V: Conclusions and Future Research

Chapter V will summarize the research and reiterate what has been learned about cloud computing and its potential applicability to DoD, specifically Army T&E. It also contains recommendations on how to proceed and identifies follow-on research that should be conducted but was outside the scope of this thesis. It also contains potential concerns, technical challenges, and cultural change that must be overcome before widespread adoption of a cloud environment will occur within DoD. The findings of this thesis combined with follow-on research will provide DoD a more comprehensive understanding of how cloud computing environments can be leveraged to improve T&E operations, streamline processes, and reduce cost.

E. KEY FINDINGS AND RECOMMENDATIONS

In this thesis, we analyzed existing processes that Army T&E users follow during the execution of a typical T&E program. We then assessed how cloud computing can be used to streamline these workflows.

In the course of documenting the Army T&E workflow processes, we focused our attention on communications and collaborations within the enterprise. This included communications starting with a request for test services, followed by scheduling a test, and compilation and delivery of a final test report (TR). The documentation consisted of use cases, activity diagrams, and collaboration diagrams for nine different scenarios. During the analysis of the current system, we determined that the current system relies heavily on e-mail and manual processes as the primary means of communication and file transport.

Currently, information is relayed in a very serial manner, with additional delay introduced whenever someone in the chain of communication is unavailable. Even though the information being requesting, in most cases, is available locally to the Test Center (TC) Test Engineer (TE) or Resource Manager (RM), ATEC does not have access to the information. In other words, storing the data locally, that is on the workstation, is an impediment to information sharing within ATEC and with ATEC's stakeholders.

Improvements could be obtained through the creation of a cloud-based integrated working environment (IWE), or “one-stop-shop,” where information could be relayed to Program Managers (PM) or other ATEC stakeholders in a more efficient manner.

The workflows could be streamlined through the use of cloud-based collaboration tools, such as: online document editors, instant messaging, threaded message boards, wikis, blogs, tags, status updates, news, hot topics, tasks, and RSS feeds. These collaboration tools, along with all collected data associated with a program, would be accessible through the IWE. The IWE would allow anyone with proper access rights to pull information relating to programs of interest from any location at any time, cross-platform cross-device, and would take the middle-man, the human-in-the-loop, out of the process. Using the IWE as the primary mechanism for collaboration would also help DoD amass the large amount of undocumented corporate knowledge employees currently posses, in their heads, into documented and searchable data.

While cloud computing is still in its infancy, this research has shown that it does bear promise to cut the cost of delivering IT services to the DoD community, other things being equal. Cloud computing is a disruptive technology whose implementation will require change across all levels of DoD. It will require technical training and a cultural shift in how DoD senior leadership, program management, end users, customers, suppliers, and especially IT professionals think about IT resources. This shift will require changes in all aspects of the acquisition of IT. In addition to the technical challenges, there will be challenges in aligning the corporate culture with the new workflows and associated means of communication and collaboration.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. CLOUD COMPUTING

1. Background

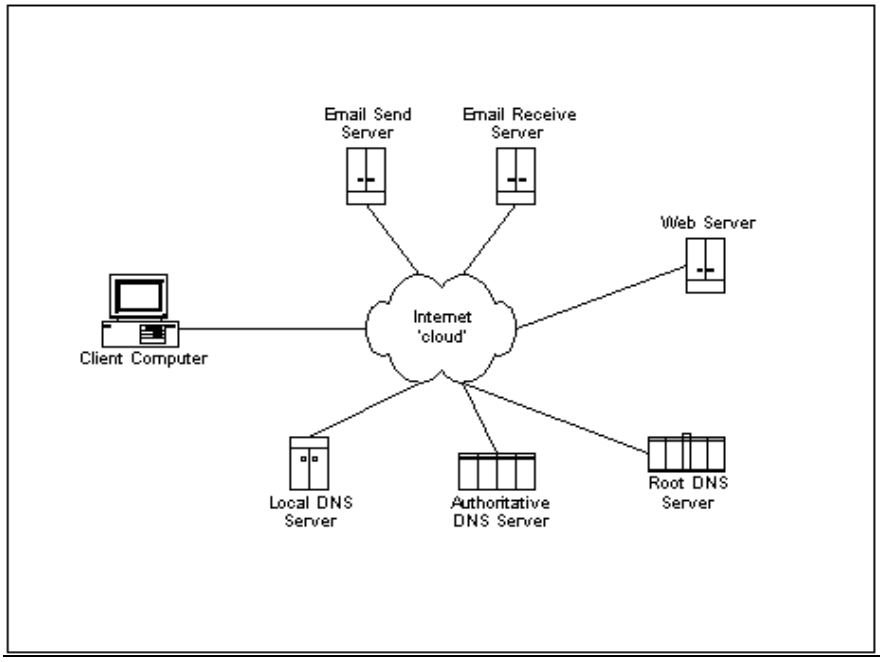

Figure 1. Typical Network Diagram from (Jeffrey, 2009)

For years, network diagrams have used a cumulus cloud to represent the Internet. The cloud image indicated something vague, intangible, but still necessary to include in the diagram. Lines on the network did nothing but travel through the cloud, indicating data passing over the Internet and no one cared where the messages went. On security-focused diagrams, the line through the cloud might include a padlock beside it to indicate that the connection is secure. The cloud has now been promoted to a first-class actor in the network diagram itself. Rather than simply passing through the cloud, lines now connect to the cloud and use it as part of an application (O'Neill, 2009). Information,

files, and applications that historically have been stored either on a user's machine or a local server are now being created, stored, manipulated, and accessed through the cloud. This makes the information accessible from anywhere and allows for the viewing of data in many different ways.

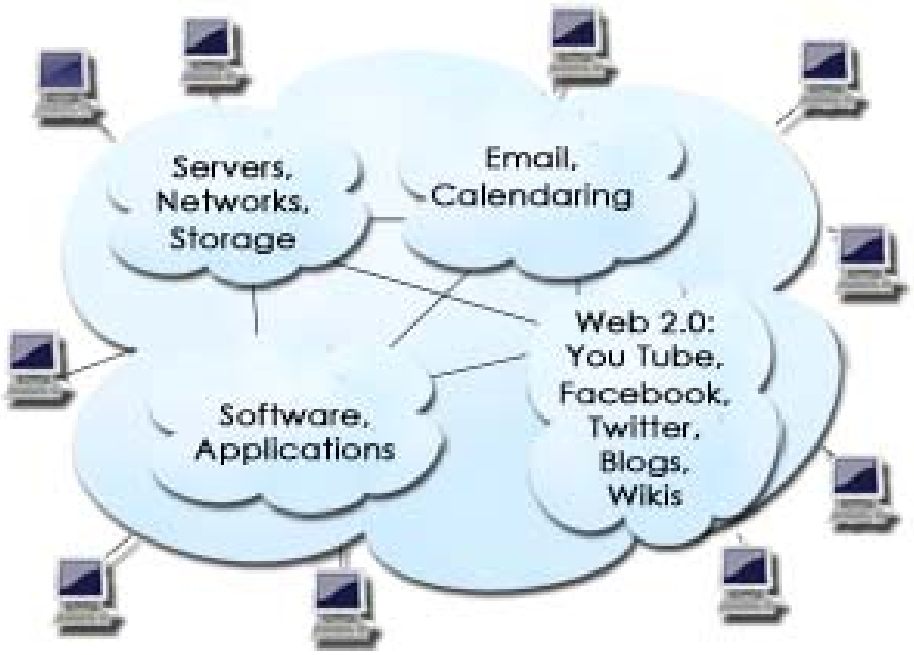

Figure 2. Cloud Computing Network Diagram from ("DOE Deploys Cloud Computing," 2010)

The model behind cloud computing is not a new or revolutionary concept. In the 1960s, John McCarthy theorized that "*computation may someday be organized as a public utility.*" (Warsh, 2006) However, only within the last few years have enough elements come together to create a perfect storm that has provided an environment in which cloud computing can flourish (e.g., technological advances, business case, Web 2.0, and economic uncertainty).

For many years, the major hurdle for cloud computing was related to the network: the available network bandwidth just did not make large scale cloud computing a viable technical solution. However, the dotcom boom of the 1990s, and resulting exponential

growth of the size of the Internet, set the stage to change this. The dotcom boom brought with it a massive investment in fiber optic and high bandwidth infrastructure, subsequently raising the percentage of the population with high-speed access to the Internet.

The business model for cloud computing was established after the dotcom crash of 2000. Prior to the crash, venture capital for startup businesses could easily be found because everyone wanted to cash in on the "new industrial revolution" (Authers & Mackenzie, 2010). However, after the stock market crashed, capital for startup businesses quickly dried up and Internet companies had to actually have a business plan. This left new startups with a tough choice. Startups could purchase servers, software, licenses, etc. that would enable their business to merely get off the ground with little excess capabilities for growth, or invest a large amount of startup capital in capabilities that may never be used. The former would work great, if the business slowly gained popularity and allowed for the ordering and integration of new hardware. However, if popularity quickly grew, traffic could overwhelm the baseline servers leading to customer dissatisfaction with the quality of service and potentially the downfall of the business. So, what is a startup company to do? Meanwhile, Internet companies like Amazon™ and Google™ were amassing great numbers of servers in large-scale datacenters to meet their businesses' peak usage demands: Amazon, to meet its ever growing presence in e-commerce and the associated peaks, such as the day after Thanksgiving, and Google to index the ever expanding Internet, while providing search results faster than its competitors. However, having enough physical hardware on hand to meet the peak usage meant that for the majority of the time this hardware would be grossly underutilized. Regardless of the utilization levels, Amazon and Google had to pay to house the hardware, power and cool it, and employ an army of technicians to maintain everything—all resulting in a large overhead operating expense for both companies.

Figure 3. Large Data Center from (“Computer History,” 2010)

By 2006, Amazon was looking at its excess computing cycles not as a fiscal drain on the company but rather as a business opportunity. Since these huge datacenters already had high-speed connections into the Internet hubs, Amazon began renting usage of its datacenter’s spare computing cycles. The offerings were quickly utilized by small companies, especially startup businesses, as this partially addressed the dilemma of having to decide how much hardware to purchase, and gave startup companies the opportunity: to access hardware in amounts that these companies would have otherwise been unable to access, only paying for what they use. Amazon and Google’s entrance into cloud computing, specifically Infrastructure as a Service (IaaS), has been compared magnitude wise to the tumultuous change that the electric industry went through in the late 19th century (Carr, 2009).

Around the turn of the 19th century, factories had to purchase customized electric generation equipment. The factory had to install the equipment and train personnel on the maintenance of the equipment. It was common for factories to hire external consultants to perform the installation and training. To upgrade the generator equipment, or change

vendors, was a non-trivial and resource-intensive task requiring preplanning. All the while, the vendors of the electric generation hardware made a large profit from reselling the same technology and services to multiple clients. This all changed when the idea of selling electricity as a utility was implemented. Economies of scale were obtained by having massive electric generating locations that could generate enough electricity to power many homes and factories. The more subscribers there were to the utility service, the higher the utilization rate of the electric generators, which in turn would lower the per unit utility rate for consumers. The lower rates made it attractive to more customers, as it now was more cost effective to purchase electricity from a utility than to generate it in-house. It has been proposed that computing is following a similar path as electricity did and that in the not too distant future computing will be offered as a utility.

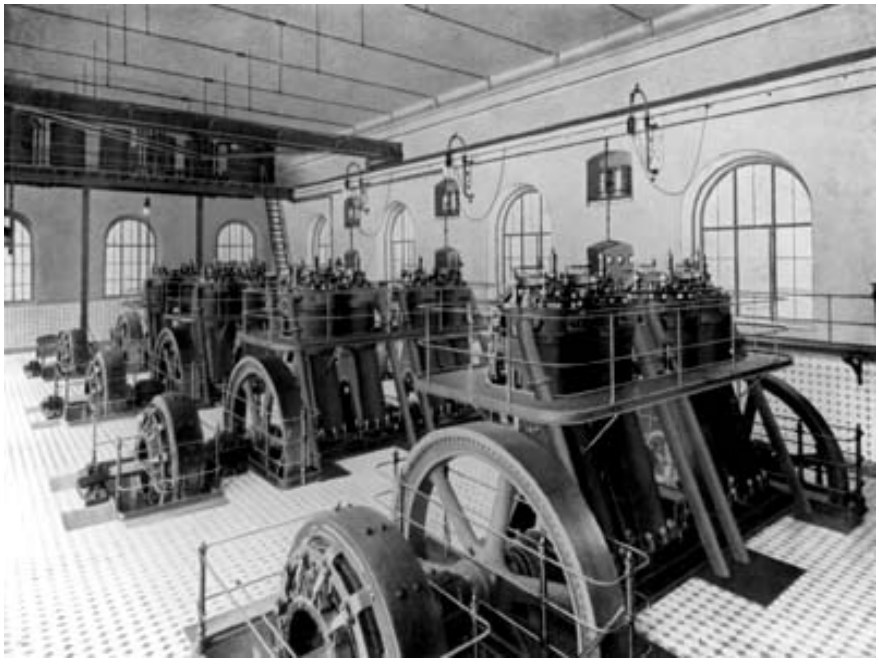

Figure 4. Power Plant circa 1904 from (Leduc, n.d.)

At the turn of the twenty-first century, Internet usage was fundamentally changing, in large part due to advancements in software development and the widespread use of standards. Software development was transitioning from a traditional institutional

form to an open source producer-subscriber concept. This decentralized approach allowed for applications to quickly be developed with Web services leading to the rise of social media. social sites, such as MySpace™, FaceBook™, YouTube™, and Twitter™, rapidly became household names. A large percentage of the population began utilizing Web-based social networking services at home and in the workplace, and became comfortable with storing and processing data at a location other than their own computer. These along with other factors, along with the economic downturn in 2007–2010, culminated in today's intense interest in cloud computing.

2. Definition

The federal CIO, charged with leveraging cloud computing, asked the National Institute of Standards and Technology (NIST) to lead federal efforts on standards for data portability, cloud interoperability, and security ("Summary of NIST Cloud Computing Standards Development Efforts," 2010). NIST serves as the government lead, working with other government agencies, industry, academia, Standards Development Organizations (SDO), and others to leverage appropriate existing standards and to develop cloud computing standards where gaps exist (Kundra, 2010). Cloud computing has been defined by NIST as:

> a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" ("Summary of NIST Cloud Computing Standards Development Efforts, 2010).

One vision of the future of cloud computing is massively scalable data centers that form a seamless infrastructure capable of remotely running applications and storing data that can be accessed from any connected device over the Internet.

Clouds offer a virtual environment for hosting user applications on one or many servers (physical or virtual) making clouds particularly compelling for applications that have unpredictable usage demands. If a company or project is not sure if they will need

five or fifty servers over the next few months, provisioning cloud services may be a viable solution. Or, if a company needs to quickly ramp up resources to handle a short spike, then a cloud can be a way to avoid investing in hardware that could be grossly underutilized for the majority of the time.

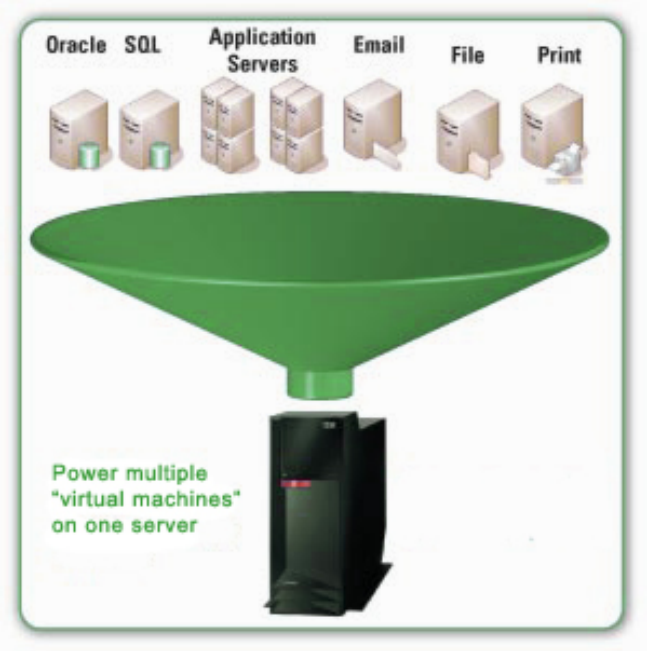

Figure 5. Virtualization from ("Server consolidation and virtualization," 2010)

Cloud computing can exist without leveraging virtualization however; users will not obtain the same level of efficiency or Return on Investment (ROI) as if virtualization were utilized. Virtualization was invented by IBM in the 1960s at a time when users were using key punches and submitting batch jobs based on a server time-sharing system (Brodkin, 2009). Virtualization, through the use of hypervisors, provided a mechanism for allowing multiple users to utilize the same mainframe through a virtual machine (VM) without risking the stability of the entire mainframe. VMs made it possible for users to deploy beta version software for testing without the need for another expensive mainframe. Virtualization is made possible through hypervisors and exokernels.

A hypervisor allows multiple operating systems (OS) to run concurrently on a single physical piece of hardware through the interception of inputs and outputs (I/O) and interrupt calls to the physical hardware. The hypervisor monitors the execution of the OS for these instruction calls and then allocates system resources (e.g., memory address ranges, CPU cycles) just as the physical hardware would, essentially cloning the physical machine. However, since multiple OSs are running on the same physical hardware, the hypervisor must keep tables mapping what resources each OS has requested and is using. That way the hypervisor does not hand out a physical resource that another OS is utilizing.

Another way to provide virtualization is to partition the physical machines' hardware giving each user a subset of the physical resources. This partition is made possible through a program, running in kernel mode, called an exokernel. The exokernal's primary function is to allocate resources to users and only allow users access to the resources that were allocated to that user. The advantage of an exokernel model is that it saves a layer of mapping. In other designs each VM has its own disk with blocks running from 0 to some maximum. The VM monitor program must maintain tables to remap disk addresses (and all other resources) whereas the exokernel model must only keep up with which VM has been assigned what resource (Tanenbaum, 2008).

VM use is not limited to servers. VMs have multiple uses within software development such as: reducing the number of OSs a developer must maintain, providing a common execution environment, and providing a deployment mechanism for preinstalled and preconfigured software. If a software package will be deployed to four different OSs, then prior to deployment the developer should test the software package out on each of the target OSs. VMs allow the developer to keep an unlimited number of different machine configurations stored on the same physical hardware removing the necessity for keeping multiple physical machines or hard drives simply for the purpose of testing. VMs can also be used on a smaller scale to provide a common execution environment regardless of the host OS. For instance, the Java programming language uses a VM called the Java Virtual Machine (JVM) as a means of ensuring that compiled

Java bytecode will execute properly regardless of the executing host OS. JVM is the environment where the Java programs execute and is the instance of the Java Runtime Environment (JRE). If implemented properly, the executing Java program can be checked for safety and executed in a protected environment, the JVM, to prevent the program from doing anything unauthorized or damaging the host OS (Tanenbaum, 2008). Just as with a physical machine, it is the software that makes a VM useful. When a VM is mixed with software you get a virtual appliance. Deploying a preinstalled and preconfigured application appliance is far easier than preparing a system, installing the application, and configuring and setting it up. A virtual appliance is not a VM, but rather a software image containing a software stack designed to run inside a VM. (Sharma, 2008).

From a server operations and backup and restore perspective, virtualization can be a tremendous timesaver. For example, the initial configuration of the operating system for a server, along with the software to run on that server can take hours, if not days, to configure. With virtualization, that initial work is done once, and the resulting standard image is saved to be deployed onto physical hardware as needed. This process can be done in as little as a few seconds to minutes and repeated as often as needed.

Regardless of how it is accomplished, virtualization allows multiple users to share hardware and software services without knowing and preferably without interfering with each other's processes. Virtualization enables a provider to present an environment to clients that appears to be completely their own environment while still gaining the economy of scale that multiple tenants provide, ("Summary of NIST Cloud Computing Standards Development Efforts," 2010) and reducing facility requirements, such as power and cooling (Carter & Rajamani, 2010).

3. Essential Characteristics

The five recognized essential characteristics of a cloud computing environment are shown in Figure 6:

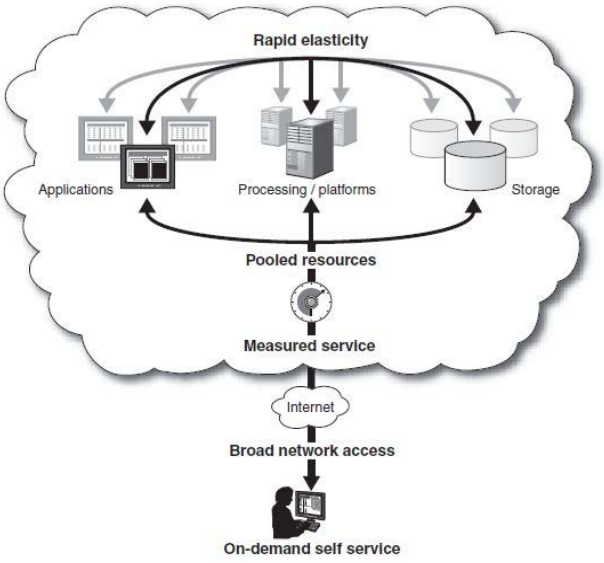

Figure 6. Essential Cloud Computing Characteristics from ("Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing," 2010)

a. Rapid Elasticity

Rapid elasticity is defined as the ability to scale resources both up and down as needed. Resources that can be scaled up or down include the number of processors, network bandwidth, storage space, or software instances needed by a client. This scaling can occur within a matter of minutes or hours instead of weeks or months. Cloud computing clients do not have to evaluate server cage, floor space, power, or cooling requirements before provisioning a new server. All they must do is provide payment for the capability that is required ("Summary of NIST Cloud Computing Standards Development Efforts," 2010). To the client, the cloud appears to be infinite, and the client can provision as many units of cloud services as needed (Jackson, n.d.).

b. Measured Service

Measured service refers to the cloud provider monitoring and controlling all aspects of the cloud service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user account).

Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service ("Summary of NIST Cloud Computing Standards Development Efforts," 2010). Tracking resource usage is crucial for billing, access control, resource optimization, capacity planning and other tasks (Jackson, n.d.).

c. On-Demand Self Service

The on-demand and self-service aspect means that a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider ("Summary of NIST Cloud Computing Standards Development Efforts," 2010).

d. Broad Network Access

Broad network access means that the cloud provider's capabilities are available over the network and can be accessed through standard mechanisms that promote use by heterogeneous thin-client or thick-client platforms (e.g., mobile phones, laptops, and PDAs) ("Summary of NIST Cloud Computing Standards Development Efforts," 2010).

e. Resource Pooling

With Resource Pooling, the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the client generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). However, this may change especially given the different treatment of security and privacy from one nation to another, and the advent of cloud computing used for processing and storing data that is sensitive to national security. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Utilization by multiple tenants is part

of what makes the “as a service” portion of cloud computing an attractive business proposition. Without multiple clients to use a service, the cost of maintaining that service, and subsequently the cost for a client to subscribe to that service, could be so large that a service provider could not make sufficient returns on investment. The ability to have multiple clients using the same platform permits economies of scale to come into play. The more clients are able to use the same platform will lower the overhead costs that are passed on to each client (“Summary of NIST Cloud Computing Standards Development Efforts,” 2010).

4. Architectures

All of the terms below share common characteristics, such as: a purchasing model of pay-as-you-go or pay-as-you-use-it, on demand scalability of the amount you use, the concept that there will be many people or multiple tenants using the service simultaneously, and virtualization (Abbott & Fisher, 2010).

The three recognized cloud architectures are:

a. Infrastructure as a Service (IaaS)

The term Infrastructure as a Service (IaaS) refers to offerings of fundamental computer resource infrastructure such as processing power, servers, storage, networking components and bandwidth as a service. This method is typically a pay-as-you-use model for what previously required either capital expenditure to purchase outright, long-term leases, or month-to-month subscriptions for partial tenancy of physical hardware. The capability provided to the consumer is the ability to provision these core computing resources such that the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls, load balancers) (“Summary of NIST Cloud Computing Standards Development Efforts,” 2010).

b. Platform as a Service (PaaS)

The term Platform as a Service (PaaS) refers to offerings of a computing platform and/or solution stack as a service. The platform typically is an application framework that typically consumes cloud infrastructure and supporting cloud applications. The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. PaaS facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers (Jackson, n.d.). The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, but the consumer has control over the deployed applications and possibly application hosting environment configurations ("Summary of NIST Cloud Computing Standards Development Efforts," 2010).

c. Software as a Service (SaaS)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from client devices through a thin-client interface such as a Web browser (e.g., Web-based e-mail). The consumer uses an application but does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities on which it is running, with the possible exception of limited user-specific application configuration settings ("Summary of NIST Cloud Computing Standards Development Efforts," 2010).

5. Deployment Models

Within clouds there is not a "one size fits all" deployment. Different companies and sectors have different requirements and concerns. NIST has theorized that there are four different ways to deploy a cloud. Each deployment model has its own characteristics, typically with varying security requirements.

The four recognized cloud deployment models are:

a. Public Cloud

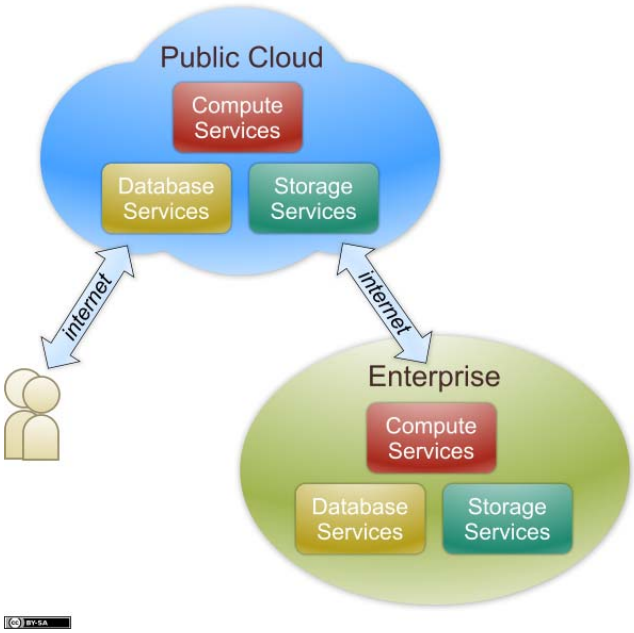

Figure 7. Public Cloud from ("Cloud Computing Use Cases White Paper v3.0," 2010)

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services ("Summary of NIST Cloud Computing Standards Development Efforts," 2010). In simple terms, public cloud services are characterized as being available to clients from a third-party service provider via the Internet. The term "public" does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user's data is publically visible; providers typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions (Jackson, n.d.). An external or public cloud is provided by an external independent entity, typically a cloud service provider.

b. Private Cloud

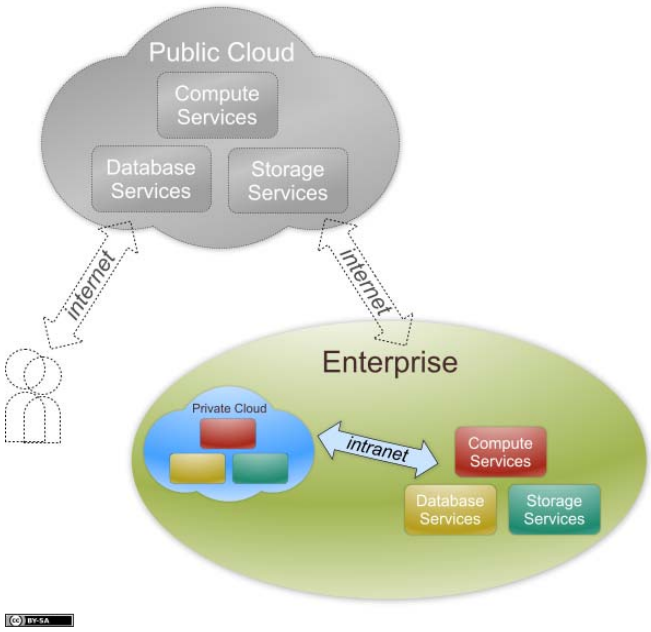

Figure 8. Private Cloud from ("Cloud Computing Use Cases White Paper v3.0," 2010)

The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on or off premise ("Summary of NIST Cloud Computing Standards Development Efforts," 2010). A private cloud is an internal deployment where cloud computing capabilities are planned, architected, acquired, and implemented to support internal business requirements (Jackson, n.d.), all while mitigating risks associated with security, privacy, legal requirements, and the relative immaturity of the cloud industry and associated technology. Private clouds offer many of the benefits of a public cloud computing environment, such as being elastic and service-based, but data and processes are managed within the organization. Private clouds offer the organization and user greater control of the cloud infrastructure, and can improve security and flexibility, because user access and the networks used are controlled by the organization. However, it is important to note that even within Private clouds communications still travel over the Internet.

c. Community Cloud

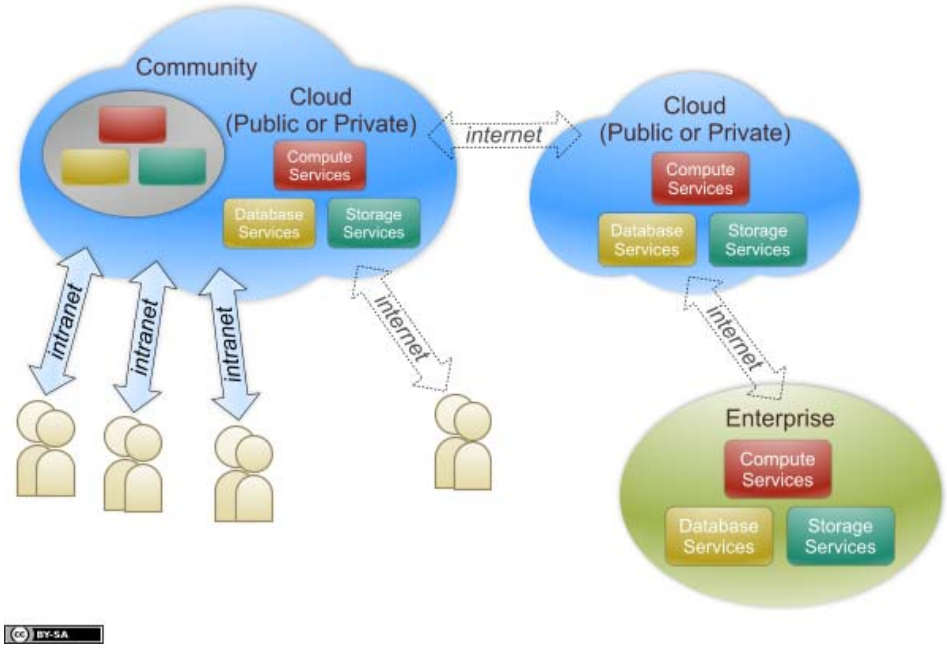

Figure 9. Community Cloud from ("Cloud Computing Use Cases White Paper v3.0," 2010)

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns or interests, such as specific security requirements, a common mission, policy, or compliancy issues. It may be managed by the organizations or a third party and may exist on or off premise ("Summary of NIST Cloud Computing Standards Development Efforts," 2010). The members of the community share access to the data and applications in the cloud. In essence, it is a semi-private cloud formed to meet the needs of a set of related stakeholders that have common requirements or interests. It may be private for its stakeholders, or may be a hybrid that integrates the respective private clouds of the members, yet enables the sharing and collaboration across their individual clouds by exposing data or resources into the community cloud (Jackson, n.d.).

d. Hybrid Cloud

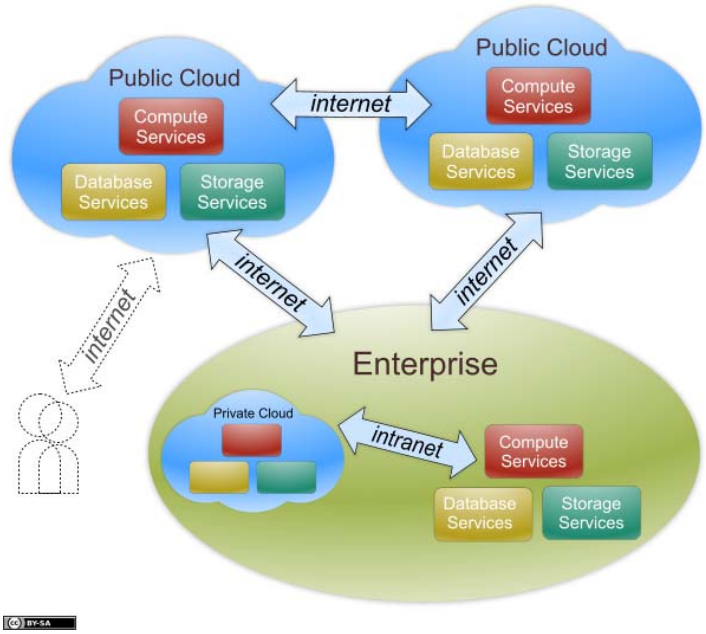

Figure 10. Hybrid Cloud from ("Cloud Computing Use Cases White Paper v3.0," 2010)

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting) ("Summary of NIST Cloud Computing Standards Development Efforts," 2010).

> Rather than throw out local applications and use the cloud exclusively, or, conversely, rely on local applications only and ignore the cloud, the prevailing wisdom is to use a combination of local applications and the cloud.
>
> (O'Neill, 2009)

Hybrid clouds typically blend a combination of internal cloud and external cloud-enabled resources that allows organizations to take advantage of the cost economics of external third-party clouds while mitigating some of the risks by maintaining an internal private cloud for critical processes and data. This hybrid approach

lends itself to an incremental deployment allowing businesses to test out the cloud while not risking everything on the success or failure of a specific vendor.

6. Government Cloud Efforts

The following sub-sections provide recent examples of how federal agencies are using cloud computing technologies. The examples presented below provide a small sampling of how cloud computing technologies are currently being used within the federal government—such as establishing a private cloud, standardizing the procurement, accreditation, and certification of cloud computing technologies, establishing a massive cloud-to-support research and moving non-critical processes to a cloud-based environment.

a. Defense Information Systems Agency (DISA) Rapid Access Computing Environment (RACE)

The Defense Information Systems Agency (DISA) provides Information Technology support to the Department of Defense (DoD). In 2008, DISA began leveraging cloud computing by creating its own secure private cloud, the Rapid Access Computing Environment (RACE). RACE provides on-demand server space for development teams through the use of virtual server technology. By using virtualization technologies, DISA has reduced the number of physical servers required to support DoD missions, and for the physical servers that remain DISA shares the operating costs amongst the users of the virtual servers. Users pay a fee for provisioning units of cloud services, which is then used by DISA to pay for the physical hardware and associated software that houses all of the virtual servers and subsequent required resources (e.g., energy, software, human resources). Within this virtual environment, users can use a self-service portal to provision computing resources in 50 GB increments with the guarantee that the environment meets DoD Certification and Accreditation (C&A) standards. The capability that RACE offers to the DoD community has reduced the server provisioning process from being at best case a multiple-week process to a mere twenty-four hour process. According to DISA, personnel can expect the same level of service and

availability when using RACE over a traditional environment (Kundra, 2010). However, if users discover that RACE simply will not meet their needs, DISA has processes in place for exiting the RACE cloud environment. DISA has established a strict data cleansing process for removing an application completely from the RACE platform. Since the inception of this cloud-based solution, hundreds of military applications including command and control systems, convoy control systems, and satellite programs have been developed or tested on RACE ("Rapid Access Computing Environment (RACE)," 2010).

b. Federal Risk and Authorization Management Program (FedRAMP)

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide risk management program, formed by the Cloud Computing Advisory Council, focused on large outsourced and multi-agency systems. FedRAMP will provide joint authorizations and continuous security monitoring of shared IT services for federal departments and agencies that enter contracts with outside providers. It seeks to create a uniform set of Federal Information Security Management Act (FISMA) compliant security standards available for leverage government-wide when procuring, certifying, and accrediting cloud computing offerings. Initially, the program will focus on cloud computing but will expand to other domains as the program matures ("Federal Risk and Authorization Management Program (FedRAMP)," 2010). FedRAMP will help lead to the development of common security requirements for specific types of systems, provide ongoing risk assessments, encourage better system integration, and drastically reduce duplication of effort and associated costs. But, perhaps most of all, it has the potential to bring a common-sense, approve-once, use-often approach that has long eluded government IT acquisitions (Kash, 2010).

These cloud security standards will allow agencies to expedite the acquisition of cloud products through the use of collaboratively developed security and accreditation baselines. The ultimate goal being to streamline the duplicative process of certifying the security of applications destined to be shared by multiple governmental

agencies. Under the current process, vendors must certify products with every agency even though each agency may have identical, or nearly identical, security requirements. This is a highly inefficient C&A model that leads to a duplication of effort both within agencies and the vendors. If FedRAMP works as intended, then cloud vendors could deliver to a single set of baseline standards, which will encourage innovation and bolster competition (Oltsik, 2010). On the government side, FedRAMP's efforts would allow agencies to reduce security compliance expenditures, expedite acquisition times, and provide consistent integration with government-wide security efforts, without sacrificing any unique security needs of their agency (Chabrow, 2010).

c. National Aeronautics and Space Administration (NASA) Nebula

Nebula, NASA's open-source cloud-computing platform, was developed to provide an easily quantifiable and improved alternative to building additional expensive data centers and to provide an easier way for NASA scientists to share large, complex data sets with external partners and the public. It consists of hardware and software housed in shipping containers at NASA's Ames Research Center. Each shipping container data center supports 100 times the file size and ten times the networking speed of the most powerful commercial cloud environment and can provide up to fifteen petabytes (one petabyte equals one million gigabytes) of storage or 15,000 central processing units (CPU) (Hoover, 2010a). Nebula allows NASA to process, store and upload thousands of high-resolution images and over 100 terabytes of data and has assisted NASA with the processing of high resolution images of the Moon and Mars for use in worldwide mapping. During this effort, data from satellites was processed and then sent to Microsoft for placement on a three-dimensional map of the world. In a traditional IT environment, new infrastructure would have to be procured in order to have enough computing and storage resources to handle the massive amounts of data. The procurement process alone would have taken months, as engineers would first need to justify why the project requires new/additional hardware/software, retrieve and supply multiple quotes, wait on an approval decision, wait on the hardware/software to be ordered and delivered, and then finally the system administrators could begin the job of

configuring the new hardware/software for use by the engineers. At the conclusion of the project, NASA would be left with a pile of legacy hardware that may or may not be able to be utilized for future projects. Through the utilization of Nebula, NASA was able to provision the virtual machines and have them up and running in a manner of hours. This ability to quickly ramp up and down allows the engineers to focus on mission-critical activities instead of IT infrastructure (West, 2010). Through the hosting of the federal government's USASpending.gov Web site, Nebula has demonstrated how a cloud-computing platform hosted by one agency can be utilized by another federal entity ("NASA Flagship Initiatives: Nebula," 2010).

Figure 11. NASA Nebula Container from ("NASA Flagship Initiatives: Nebula," 2010)

In addition to expediting the process of standing up resources for new efforts, Nebula also assists NASA with addressing a side effect of having decade-long missions, keeping servers and data acquisition systems under configuration control. Since

NASA space exploration missions can take over ten years to develop, the resources needed to process the data coming back are usually scheduled and procured well before launch and placed in a configuration lock down. Missions, however, can be delayed at a late stage, cancelled altogether, or last much longer than originally anticipated leading to IT infrastructure, which is not needed or is required, to be in configuration control for longer than expected. Nebula's cloud services allow NASA to be much more flexible and responsive to actual mission needs, scaling resources up or down as the actual requirements of the mission develop.

Currently, Nebula is an IaaS implementation allowing IaaS customers to unilaterally provision, manage, and decommission computing capabilities on an as-needed basis through a Web interface or set of command-line tools. NASA plans to begin offering a PaaS in late 2010 and a Database as a Service (DaaS) in 2011.

d. Department of Energy (DOE) Cloud Computing Migration

The Department of Energy is exploring cost and energy efficiencies that can result from leveraging cloud computing. The Lawrence Berkeley National Labs (LBL) initiative is exploring how to use cloud computing to address needs across the enterprise, in specific business services and in scientific study. According to the DOE CIO: "*LBL has deployed over 2,300 mailboxes on Google Federal Premier Apps, and plans to have 5,000 e-mail accounts deployed by August 2010. This solution uses a LBL Identity Management System to provide authentication*". LBL small and medium sized scientific research teams are also utilizing Google Docs and Google Sites to foster collaboration and community documentation. LBL estimates the deployments that have already been made will save $1.5 million over the next five years in hardware, software and labor (Kundra, 2010).

e. Department of Interior (DOI) Agency-wide E-mail

The Department of the Interior is pursuing a SaaS cloud computing model for e-mail. DOI has 80,000 e-mail users who are widely dispersed across the United States and are currently supported by a complex messaging infrastructure comprised of

more than a dozen different e-mail systems. "*By implementing e-mail using an external commercial SaaS model, the department expects to provide improved service to its 80,000 users for one-third the amount of money that it spends today*" (Kundra, 2010). The department is moving forward with this project with an anticipated completion date in Fiscal Year 2011.

7. Cloud Concerns

Figure 12. Stormy Road Ahead from (Price, 2007)

Although cloud computing promises to provide enterprises and IT with relief from numerous pain points, utilizing cloud deployment methods, either individually or in combination, significantly alters an organization's risk profile (Christiansen et al., 2010). Moving to a cloud-based environment may not be appropriate in all circumstances, and whether it is a viable option will depend on how it is used and how many risks can be mitigated. Just as with any other new technology or service, moving to a cloud environment should be done in a careful balanced way and only after thorough planning, research, risk assessment, and pathfinder pilots have been performed. Business goals should be defined, a risk-benefit analysis should be performed to determine whether moving to a cloud is applicable, worst-case scenarios should be examined to identify

what processes are jeopardized, and contingency plans should be created for each scenario, e.g., scenarios such as what happens if there is a security breach or what happens if the cloud is unreachable for various lengths of time. The section below lists some of the many areas of concern that potential cloud adopters should investigate prior to moving to the cloud.

a. Security

First instincts when outsourcing control and processing of data is to be concerned that doing so will lower an organization's overall security posture; however, that may not always be the case. Cloud computing has the potential to enhance security while also introducing additional vulnerabilities. In most organizations, security is either understaffed or is another duty as assigned and not the primary competency of the IT staff. Additionally in the past, keeping data secure was much less challenging than it is today. File formats were likely proprietary, data was placed in silos, relationships between data producers and consumers were closely coupled, and fewer people worldwide had access to technology. Today organizations could potentially obtain better security by moving to a cloud environment where the provider has dedicated security personnel whose sole mission is to secure the cloud infrastructure (Robert Mullins, 2010). From a patching standpoint, cloud computing holds the potential to drastically change the losing game of continual patching and IT device remediation through the distribution of standardized locked down machine images (Gourley, 2009). Through the use of virtualization and automation, cloud computing will expedite the implementation and deployment of secure configurations for VM images. When vulnerabilities are detected, they could be managed more rapidly and uniformly.

Conversely, having a private DoD cloud could also lead to increased coordinated attacks on the cloud. Due to the high collection of data within a cloud, a DoD private cloud would create an extremely high-profile target for hackers, foreign states, and terrorist organizations. When you put more eggs in one basket, the prize for breaking into the basket becomes much larger. If a DoD cloud were successfully breached, then the attacker could move laterally and capture more information than if a single

installation were breached. From a national security perspective the amount of damage that could be inflicted on the DoD via spyware, botnets, or other malicious programs is magnitudes greater than in non-cloud environments. Thus it is important that all security policies, processes, procedures, and controls in place have been implemented properly. From an adopter's standpoint, it is important to understand what these security policies are, what the incident response is in case of a breech, what type of physical security is in place, what data protection measures are in place (such as data encryption at rest and in-motion), what type of logging and auditing are employed, how information leakage is prevented, how data is segregated in multitenant situations, how data is destroyed after removal from the cloud (e.g., backups), how root user access is controlled, who all has access to the data, and so on.

Due to the fluid nature of cloud computing, it is difficult to even determine what questions we should be asking to improve the security and privacy that clouds can afford. However, a few of the many questions and issues related to providing security assurances within a cloud environment follow. (Dinolt & Michael, 2010) Fundamental questions should be addressed such as whether current architectures are adequate for building trusted clouds, or if new architectures are needed. Whether current OS and application security approaches will scale properly to a cloud computing environment, or if new approaches will need to be taken to provide a trusted OS. Efforts are currently underway within the Naval Postgraduate School (NPS) to investigate the security policies, models, and appropriate architectures to address the OS and architecture questions. More detailed information regarding NPS's research can be found in the DoD IAnewsletter article titled "Establishing Trust in Cloud Computing". (Dinolt & Michael, 2010)

Since users and developers are still discovering new ways to apply cloud technologies, generating new expectations surrounding security and privacy, it will be difficult for organizations to assess and manage risks. The cloud and security communities should establish a common set of 'best practices' for cloud based security policies/models, addressing items such as: data integrity, protection of personally

identifiable information, data destruction, communications security, privacy, authentication, and so on. Several vendors have formed the Cloud Security Alliance (CSA), which is promoting independent research into best practices for cloud computing security. These communities should also address how to provide checks and balances to ensure that security resources are correctly implemented and maintained in the cloud. The best practices mentioned above could be used by customers in evaluating the offerings of various vendors. Providers must find the fine line between supplying customers with enough transparency into security protections and procedures to alleviate concerns, while not providing so much transparency as to assist malefactors. This transparency begins with the service-level agreement (SLA).

b. Service Level Agreement (SLA)

An SLA is part of a service contract where the level of service is formally defined between a provider and a customer. SLAs are common in network services and typically measure the parameter set known as quality of service (QoS). It is important to note that while SLAs are important they cannot guarantee acceptable performance, SLAs can only punish failure to perform as promised. The more detailed an SLA is the better. Typical items specified within an SLA include pricing, processes and procedures, business continuity requirements, reliability, data safety, security, availability, maintainability, performance benchmarks, provisioning turnaround times, geographic restrictions, encryption requirements, system uptime, resiliency, responsiveness, emergency contacts, clauses that spell out the rights and responsibilities of the provider and customer, and last but not least, violation recourse (Milburn, 2010).

However, current commercial cloud implementations do not offer adequate SLAs, their control tools, or machine-actionable SLAs yet. The SLAs do not offer safety audit processes or regulations for storage and backup of data that is managed in the cloud (Cueli, 2010). Another stumbling block for cloud computing SLAs is that enforcement will be difficult because of the shared nature of cloud computing (Avoyan, 2010). If QoS issues arise, it will be extremely difficult to determine the root cause for service interruptions due to the complex nature of the shared resources (e.g.,

infrastructure, platform, software) each of which are integral to the end users' experience. In a cloud environment, it may be difficult to determine who should be held accountable for the service interruption.

c. Standards and Data Portability

Cloud adopters, both public and private, must be able to easily store, access, and process data across multiple clouds; weave together a mesh of different services to meet their needs; and have a way to collaborate with business partners around the globe. However, without security, management, data federation, and multi-tenancy standards cloud interoperability will not be fully realized and adopters will experience vendor lock-in. Currently, there are several ongoing efforts within focus groups, nonprofits, and standards bodies to create community-recognized standards for cloud computing. Groups, such as NIST, CSA, and the European Network and Information Security Agency, are all working on cloud computing standards. Without these standards, there will also likely be Application Programming Interface (API) and platform lock-in. Without formal standards, de facto standards will arise from vendor and customer interactions; for instance, software giants Microsoft and Oracle have indicated that they will press on with developing cloud solutions regardless of lock-in and let standards catch up down the road, if they can (Clarke, 2010).

Before moving to a cloud environment, organizations should have a well-documented entrance and exit strategy for critical data and business processes. Distinct strategies should exist for importing and exporting data into vendor-specific software, transforming data formats to and from formats supported by the vendor, and for transitioning business processes from a traditional environment to and from a potentially proprietary-cloud based format (DiMaio, 2009). Any organization that moves data, and more importantly business processes performed in embedded software services, into a cloud-based environment should develop an exit strategy. If the move to the cloud does not work as expected, organizations should have a well-defined process for retrieving both their data and business processes out of the cloud and returning it to a traditional environment (Prigge, 2010). This involves knowing what the cloud provider requires to

remove data from its cloud (such as RACE's strict data cleansing process), whether the provider has any utilities to assist with removing the data, whether the data will need to be transformed from one format to another, and whether the provider will charge for assisting with the removal of the data from the cloud.

8. Steps to Cloud Nirvana

Moving to a cloud environment is not merely about obtaining cost savings and efficiencies of scale with hardware and software, the low-hanging fruit. The move is also about removing unnecessary constraints tying users to specific hardware, software, and workflows leading to increased user productivity. Cloud computing has the potential to change computing from being application-centric to a data-centric view of information processing. Those pursuing cloud computing should focus on reaching the high-hanging fruits, the removal of unnecessary constraints surrounding the storage, retrieval, and manipulation of data-objects, a state called 'cloud Nirvana'. In cloud Nirvana any object created on one computing device (e.g., desktop, smartphone, tablet) will be accessible from any another computing device regardless of how the object was created or what application is opening the object (Foster et al., 2010a).

Changing to a data-centric view has the potential to fundamentally change computing just as other past innovations have, such as: modems, laptops, the Internet, and mobile computing changed the usage of the technologies of their respective era. For instance, modems by allowing multiple users to utilize a mainframe from offsite, laptops by allowing users to take applications and data with them, the Internet by allowing access to email and other corporate software from anywhere, and mobile computing devices (e.g., smartphones, tablets, laptops) by allowing users to access repurposed content from internet enabled devices.

While documenting a roadmap for reaching a cloud Nirvana is not the focus of this research, it is important to introduce the initial high-level stages (Migration, Integration, and Unification), which need to be accomplished before Nirvana can be realized.

> The Migration stage involves the movement of existing data and applications from various sources to the cloud, and the merging into an integrated working environment (IWE).
>
> The Integration stage aims for a working environment that provides an integrated tool for collaboration and communication activities and involves merging, or purging, of unnecessary duplication of both data and applications.
>
> In the Unification stage we leverage the cloud environment to the ultimate level of collaboration and communication – the unification of the workload. The final boundaries between the data and application are removed leading to an information-centric environment. Rather than having data and applications we have artifacts, which are embodiments of data and their associated manipulators, mini programs that allow the user to process (e.g., view, edit, and print) the data (Foster et al., 2010a).

For additional information regarding research into realizing a cloud Nirvana, please reference the article: "Removing the Boundaries: Steps Toward a Cloud Nirvana" in the August 2010 edition of IEEE International Conference on Granular Computing (Foster et al., 2010a).

B. USE CASE ANALYSIS AND METHODOLOGY

1. Definition and Overview

Use cases are useful in capturing and communicating functional requirements by capturing who (actor) does what (interaction) with the system, for what purpose (goal), without dealing with system internals (Malan & Bredemeyer, 2001). A complete set of use cases specifies all the different ways to use the system, and therefore defines all behavior required of the system, bounding the scope of the system.

Use cases are used in software engineering to identify, clarify, and organize system functional requirements (intended behavior of the system) in an easy to understand manner. Generally, use case scenarios are written in an easy-to-understand structured narrative using the vocabulary of the domain (Malan & Bredemeyer, 2009). This makes it easy for users to follow and validate the use cases, and the accessibility encourages users to be actively involved in defining system requirements. Use cases are initiated by a user with a particular goal in mind and contain all system activities and

possible scenarios that are of significance to the users. The system is treated as a “black box” with all interactions, including responses, being perceived as coming from outside the system.

Use cases describe the sequence of interactions, and potential variants of this sequence, between external actors and the system under consideration necessary to satisfy the goal. Actors are parties, outside the system, that interact with the system and may be a class of users, roles users can play, or other systems (Cockburn, 2000).

A use case, or set of use cases, has the characteristics below ("What is a use case?," 2008):

- Describes one main flow of events, and possibly variants of this flow
- Is multi-level, so that one use case can use the functionality of another one
- Models the goals of system/actor (user) interactions
- Organizes functional requirements
- Records paths (called scenarios) from trigger events to goals

III. CURRENT T&E PROCESS

A. INTRODUCTION

Tracking and maintaining situational awareness of documents, presentations, and other types of business-driven data is difficult even in small organizations in a single location. Naturally, the efficient management of this type of information becomes more difficult in large organizations such as the Army Test and Evaluation Command (ATEC), with thousands of users and multiple physical locations. From a program management perspective, inefficient management of this information leads to stale data upon which to base decisions. From an IT management perspective, inefficient management of data results in unnecessary infrastructure costs.

This chapter provides a high-level mission scenario of the current process for program management, test reporting, and range-test scheduling within ATEC. We first provide an overview of the ATEC domain, followed by a walkthrough of a typical scenario for acquiring and conducting live-fire tests of a system. We document the scenario by using use cases, activity, and collaboration diagrams. These artifacts are used in Chapter IV to motivate the discussion of how cloud computing in its current form could meet the needs of the Army T&E community. The selected use cases were chosen as they could easily be extrapolated to other domains, as every DoD domain will have program management, report collaboration, data storage, and resource-scheduling requirements. The use cases in Chapter III and Chapter IV are based on the same high-level mission scenario.

B. OVERVIEW OF THE ARMY T&E COMMAND DOMAIN

1. Background

Title 10 of the U.S. Code requires that major acquisition programs undergo independent operational test and evaluation (OT&E) in order to proceed beyond low-rate initial production (LRIP) ("DoD Instruction 5000.02", 2010). The intent of the law is to establish a system of checks and balances that will ensure that soldiers in the field are

equipped with the best possible equipment (Johnson, 2003). The three U.S. military departments have all undertaken initiatives to link the tests of systems under development with the operational tests that involve test exercises in the field. To facilitate this initiative, the Army reorganized its T&E program in October 1999 to place developmental and operational testing under one command, ATEC.

ATEC plans, conducts, and integrates developmental testing, and independent operational testing, independent evaluations, assessments, and experiments in order to provide essential information to acquisition decision makers. ATEC is comprised of three subordinate commands: Developmental Test Command (DTC), Army Evaluation Center (AEC), and Operational Test Command (OTC) each with a different focus ("U.S. Army Test and Evaluation Command," 2010) see Figure 13.

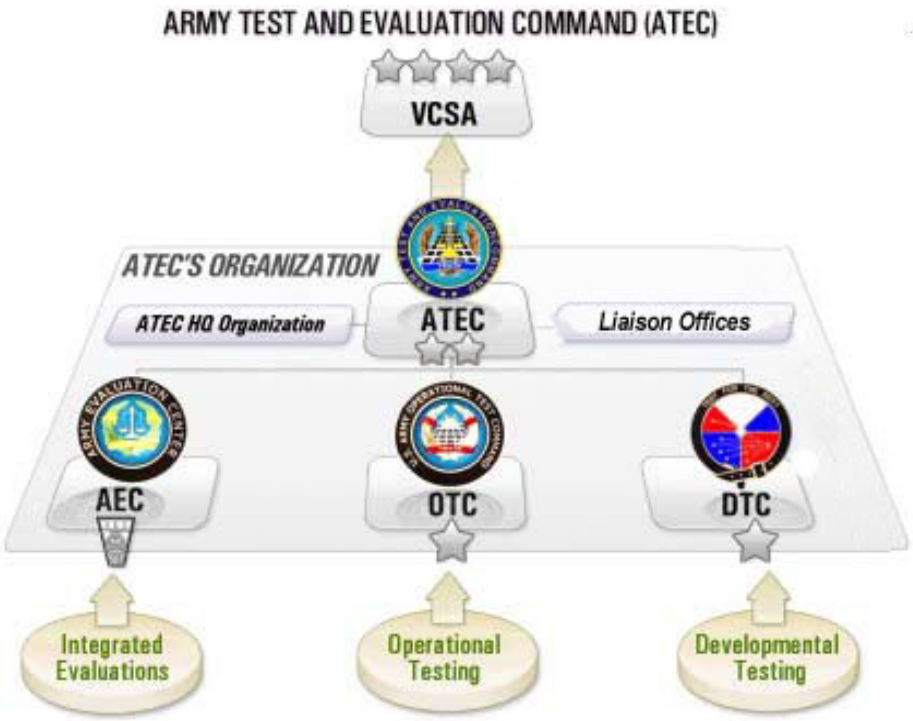

Figure 13. Army T&E Domain from ("U.S. Army Test and Evaluation Command," 2010)

a. Developmental Test Command (DTC)

DTC is the technical tester for the ATEC. DTC tests military hardware and software of every description under precise conditions across the full spectrum of arctic, tropical, desert, and other natural or controlled environments. DTC provides a full range of test services, including providing unbiased test data on the technical feasibility of early concepts, determining system performance and safety, assessing technical risks during system development, confirming designs and validating manufacturers' facilities and processes at both system and component levels. DTC offers its testing capabilities to all U.S. military services and DoD organizations, along with federal agencies, state and local governments, foreign and allied governments and private industry ("U.S. Army Developmental Test Command," 2010).

b. Operational Test Command (OTC)

Following developmental testing and issue of a safety release, a piece of equipment is delivered to the OTC for independent OT&E. OTC's mission is to conduct realistic operational testing with representative soldiers and units in the areas of equipment, doctrine, force design, and training. To perform this mission OTC plans, conducts, and reports operational tests, assessments, and experiments in order to provide essential information for the acquisition and fielding of warfighting systems. Ultimately OTC is responsible for ensuring each piece of equipment is operationally tested before being placed in the hands of warfighters ("U.S. Army Operational Test Command," 2010).

c. Army Evaluation Center (AEC)

AEC provides the evaluation portion of ATEC's T&E mission. AEC plans and conducts independent evaluations and assessments of acquisition programs providing the results to DoD decision makers and soldiers. AEC evaluates the data obtained from DTC, OTC, contractor testing, and modeling and simulation (M&S) events to determine a system's operational effectiveness, suitability, and survivability. AEC is the organization that writes the final report, System Evaluation Report (SER), used by the

decision makers to determine whether a new or enhanced system will be fielded and become part of the Army's arsenal ("U.S. Army Evaluation Center," 2010).

2. ATEC Enterprise

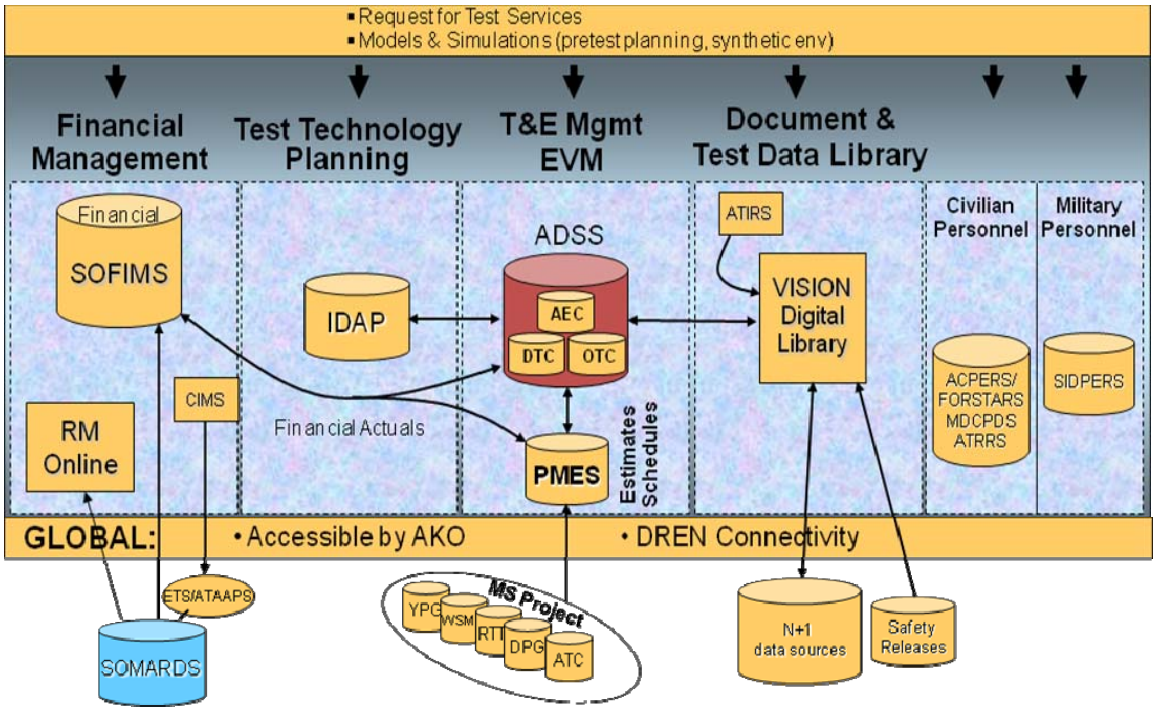

Figure 14. ATEC Enterprise Notional High-Level System View (circa 2006)

Within the ATEC Enterprise (Figure 14), there is a need for a consolidated program management and test reporting system. Currently, ATEC and its subordinate commands have numerous stovepipe systems and workflow processes, which at best, awkwardly communicate program status to customers and ATEC leadership. Through the use of a private cloud, the current process could be replaced with a more automated process allowing customers, leadership, and other stakeholders to pull information as needed in an automated fashion rather than manually contacting the local test center point of contact (POC) to obtain that information. Systems, such as the Standard Operating and Maintenance Army Research and Development System (SOMARDS), SOMARDS Financial Information Management System (SOFIMS), ATEC Decision Support System (ADSS), Versatile Information Systems Integrated On-Line (VISION) Digital Library

System (VDLS), and Performance Measurement Enterprise System (PMES) are all involved in the current program management and test report generation/delivery process, as depicted in Figure 15. A description of each of these systems follows.

a. SOMARDS

SOMARDS is the Army's authoritative financial management and reporting system that maintains all actual financials and is used by the Army to collect, manage, and distribute funds. It provides for reimbursable customer and direct mission funds control, reporting for labor, reimbursable billings, advances, and general operating expenses. Particular features include: on-line and batch processing; general ledger reporting; production of daily, regulatory, and monthly reports; file inquiry/maintenance capability; and month-end/year-end and purge processes.

b. SOFIMS

SOFIMS is an internal ATEC system that performs daily imports from SOMARDS. SOFIMS restructures SOMARDS information from each update in order to present information in a format that is easier to use by ATEC customers than SOMARDS. It provides financial execution information, commitments, obligations, costs, and disbursements relative to both direct and reimbursable dollars received by the command. It allows users to store, sort, search, and present command-wide financial information in a user-customizable manner.

c. ADSS

ADSS is ATEC's Web based T&E planning tool that tracks the resources (e.g., equipment, labor, dollars) that are required to conduct a test or evaluation. It is used as a comprehensive management system to track, record, and monitor T&E planning, execution, and reporting for all ATEC T&E activities. It contains all system T&E information including ATEC System Team (AST) membership, program schedules, T&E schedules, cost estimates, funding requirements, and document status and dates for all of ATEC's T&E projects. ADSS is the official repository for tracking all Developmental

Test (DT), and Operational Test (OT) projects that identify resources (e.g., units, personnel, ranges, equipment) for tests requiring soldier support. ADSS also provides a single source for requesting DTC test services and provides its own estimated financial data by pulling in actual financials from SOFIMS on a daily basis.

d. VDLS

VDLS is a Web-based knowledge management system that provides distributed information management capability supporting information fusion. VDLS provides access control so that information is protected and provided to only those users with the required access permissions. VDLS provides users a place to store and access information from any place that has an Internet connection. VDLS is ATEC's primary business tool for the collection, management, and timely dissemination of data and information for decision making. When an ADSS test project becomes active a test project shell is created within VDLS. The project shell is the mandated repository for the interim data report, final test report, test record, and all level-three and above test data. A repository for level-one and level-two data does not currently exist; for a description of the seven different levels of T&E data see Table 10 in Chapter IV.B.

e. PMES

PMES provides the ability to retrieve and display accrual data directly in Microsoft Project for analysis and reporting purposes. If this information is updated regularly, users should be able to analyze spending patterns over time in the context of a project's estimated spending plan. ADSS provides the central repository and other functionality, which allows PMES to serve as a single T&E program management system. Currently, PMES is only deployed to a few ATEC pilot locations so its usage is not widespread.

C. TYPICAL T&E MISSION THREAD

A program is a set of projects that are managed together to achieve a common goal. Programs are typically large undertakings that require integrated management of the

individual projects that make up the program. A project is a temporary endeavor, having a defined beginning and end. It is undertaken to meet unique goals and objectives in order to deliver specific outputs usually bringing about beneficial change or added value (Nokes, 2008). An individual DTC, AEC, or OTC weapon test could be considered to be a project with the delivered product being the respective final test report. The entire coordinated set of DTC, AEC, and OTC projects for a specific weapons platform comprise a program. At ATEC, the typical system evaluation is structured as a program with AEC, DTC, and OTC each managing their respective pieces but in coordination with each other.

Program management is the discipline of planning, organizing, and managing resources to bring about the successful completion of specific project goals and objectives, as shown in Figure 15. Program management emphasizes the coordination and prioritization of resources across projects, managing links between the projects, and managing the costs and risks of the program.

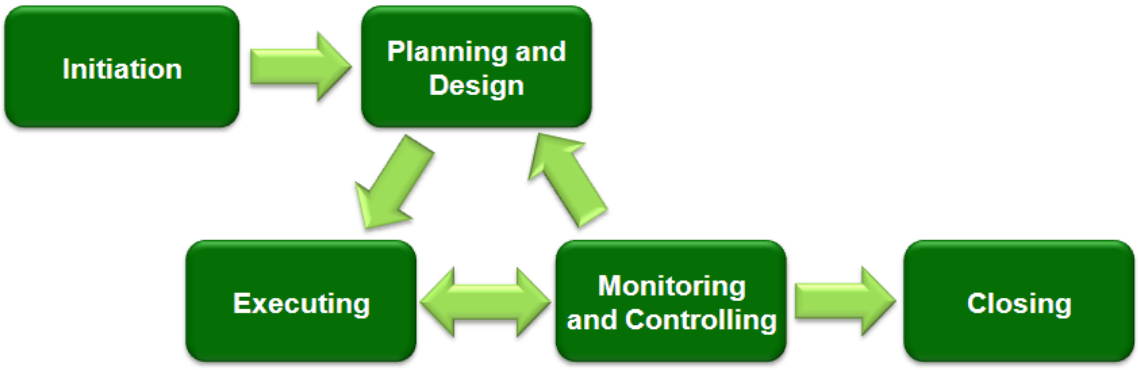

Figure 15. Program Management Steps from (“Management Steps Part 3,” 2009)

ATEC does not currently have a comprehensive standard way of performing program management. Program managers (PM) are not able to properly monitor the current status of projects within their program. As a result the program manager, and ultimately ATEC senior leadership, may be making decisions based on incomplete or outdated information.

The current system provides monitoring at the milestone level, which only reflects a snapshot in time of the project status. Utilizing external task relationships and consolidated projects with Microsoft Project enables the program manager or AST Chair to coordinate and view a program schedule. However, the current implementation does not allow the PM to drill down to the actual range schedule, as only the milestones are currently available. This is due to the multiple semi-stovepipe systems that comprise the ATEC Enterprise, as shown in Figure 14.

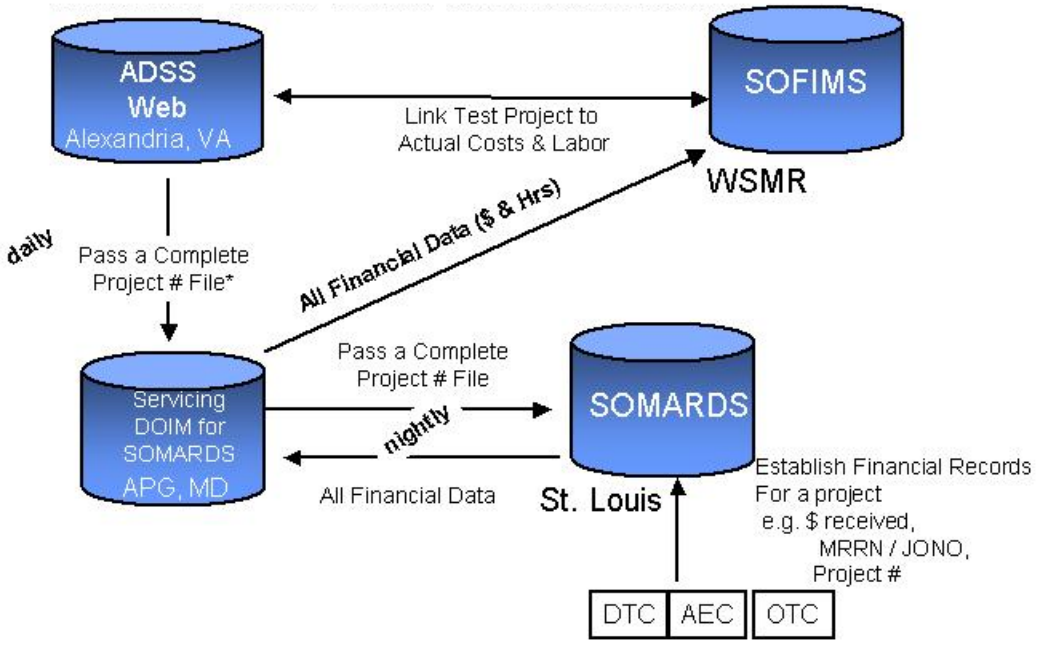

Figure 16. ADSS SOFIMS SOMARDS Integration

The ATEC-specific SOFIMS pulls financial information from SOMARDS (Figure 16). Test milestone and rudimentary schedule information is stored in ADSS with milestones being pushed into SOFIMS. Level 3-plus data—test reports of record—are stored within VDLS in a folder structure based on the unique ADSS number and milestones within the ADSS schedule. All of the previously mentioned tools are primarily used at the ATEC HQ level for tracking expenditures and the health of a program based on high-level goals. However, at the test centers (TC) where the testing

actually occurs there are more specific tools, such as: multiple unique range scheduling systems that are used by range personnel to schedule tests, deconflict safety fans, deconflict air or ground space, and track meta-data about the test, such as serial numbers and test setup information. Also, at the local test centers there are data storage systems that store everything from the raw collected test data to the final level-three test report.

A safety fan refers to the surface danger zone (SDZ) for the SUT. SDZs represent the minimum safety boundary surrounding a live fire test event, and are unique for each range and SUT. "The objective of a SDZ is to represent the residual risks of fragment escapes or other danger to the public at no greater than 10^{-6} (one in a million)" (Army, 2003).

1. Program Management

After completing a test for an evaluated system at any of the ATEC TCs, a process similar to the one shown in Figure 17 and the corresponding collaborations shown in Figure 18 occur. For non-evaluated systems the process is a subset of the evaluated system.

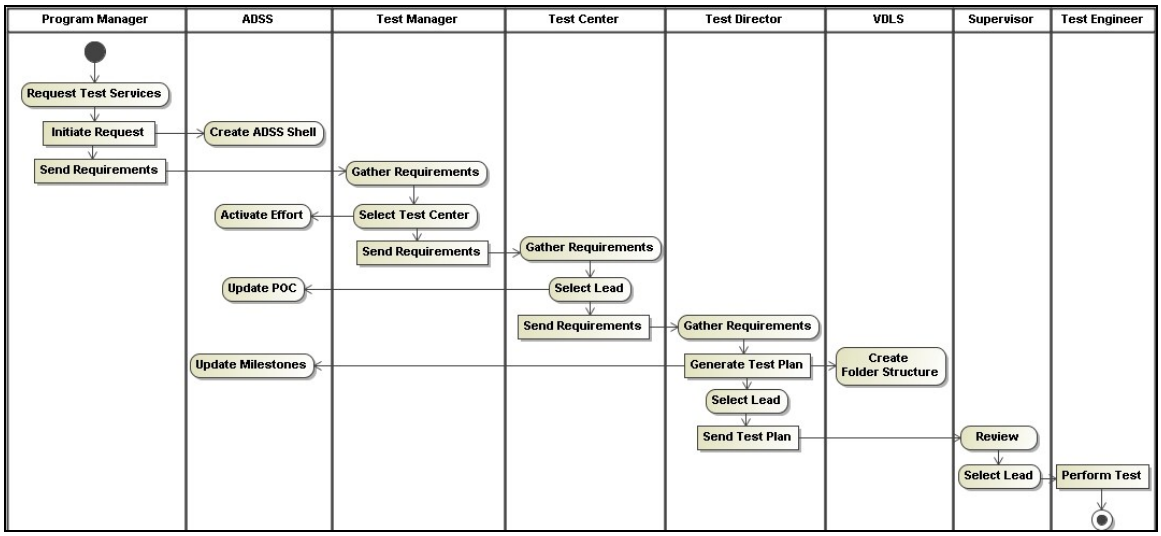

Figure 17. Program Management Process

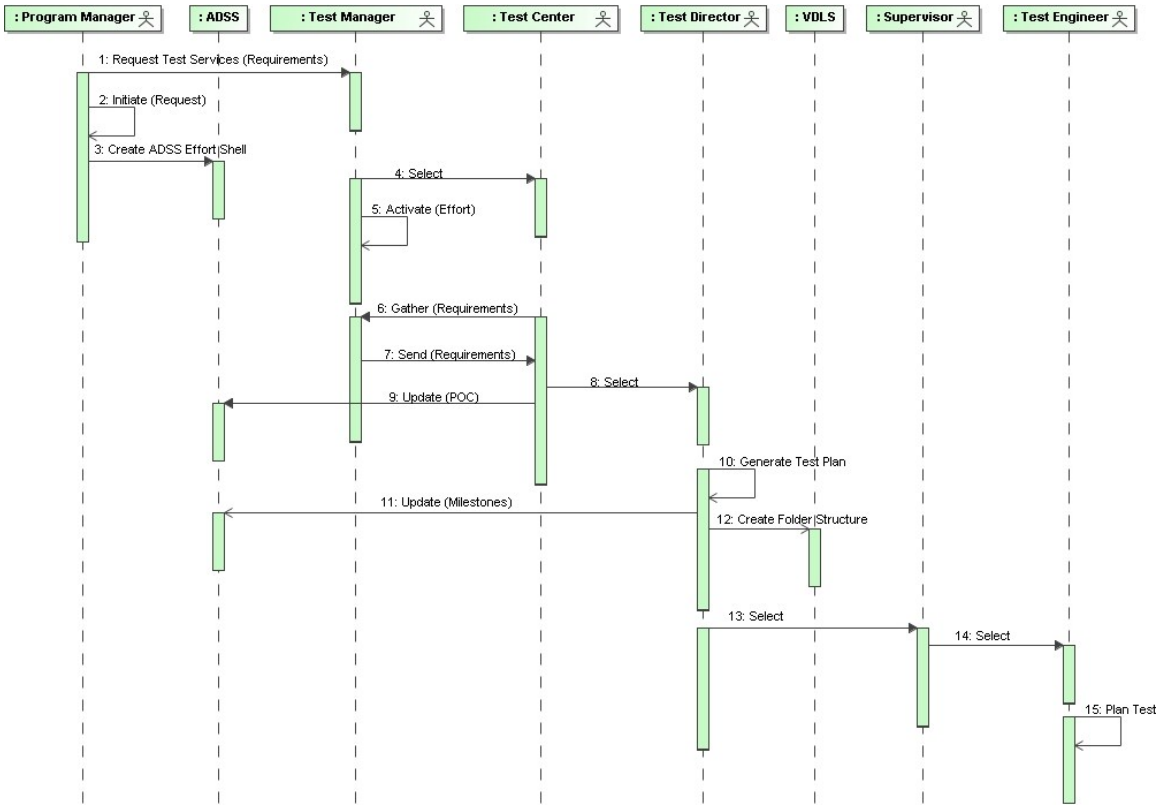

Figure 18. Program Management Collaborations

The primary scenario used throughout the remainder of this research deals with an evaluated system, although a non-evaluated system would utilize a subset of the same processes. Prior to full production of a new weapons platform a PM decides to split LRIP between multiple contractors for the mandated Live Fire Test and Evaluation (LFT&E) portion of the test program. This is also known as a contractor fly-off and is done in an effort to obtain the best value choice for the government. A fly-off allows the government to keep competitive forces working for a longer period of time and make final decisions based on information that is as realistic as possible. It provides the government an opportunity to reduce the risk that a single source contractor will not deliver a product that meets the requirements as the government can pick the best delivered LRIP product based on hard requirements and evaluation criteria.

When an external customer or ATEC organization requires ATEC services, the responsible party submits a Request for Test Services (RFTS) to formally initiate the

request. The PM submits a Request for Test Services (RFTS) to ATEC to establish a test program. After the RFTS has been submitted, ATEC will Initiate the request, creating an ADSS Effort Shell (Effort), and then forward it to the appropriate DTC Test Manager (TM). The final step in the ATEC project initiation process is to create a plan in Microsoft Project to support detailed planning and estimation. This project plan will be created using PMES and the initial project plan will contain all of the milestones and other information that was accumulated during the previous steps.

The DTC TM then determines which TC is best suited to accomplish the testing requirements, activates the effort, and forwards the request to the selected TC. Throughout the request distribution process, DTC HQ, DTC TM, and the TC may add and edit milestone information contained within the effort. Upon receipt of the effort, the TC assigns a Test Director (TD) to coordinate all local tests, generate a test plan, and manage the effort. This assignment is officially recorded within ADSS in the TC POC field.

2. Conduct Test Process

The TD then, based on the initial test plan requirements, distributes and coordinates the various stages of testing to the TC functional directorates (e.g., Missile Performance and Sensors, Aviation, Environmental and Component) where a Test Engineer (TE) is selected to actually conduct and manage the day-to-day status of testing. Each selected TE is responsible for either performing or coordinating all aspects of their portion of the test plan, covering everything from pretest test planning, test execution, post test analysis and data verification, to collaboratively authoring the final test report (TR).

a. Pretest Setup Process

Pretest coordination is necessary because conducting a test is potentially a destructive process and costly process. The coordination is done for safety and to ensure that all test data is captured the first time, every time. That way the test does not have to be repeated at a later date due to poor planning. Figure 19 shows the pretest planning and setup process.

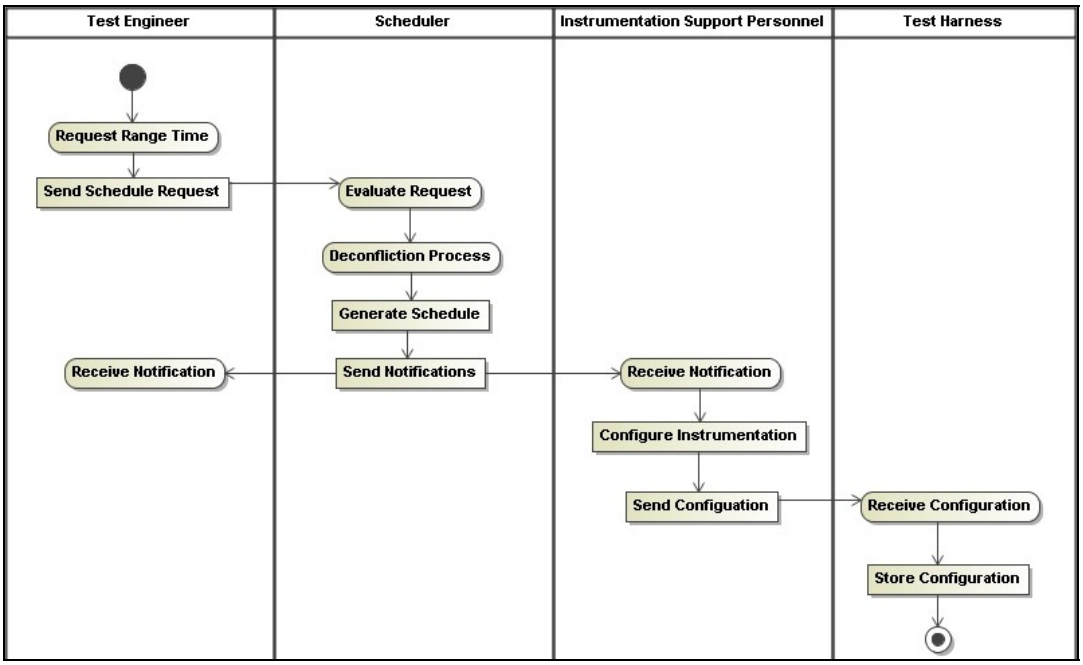

Figure 19. Pretest Setup Process

During pretest planning, the TE verbally socializes the system under test (SUT) anticipated test dates with other co-located TEs and range personnel to determine if the dates will cause any unavoidable conflicts. The TE also works with Instrumentation Support Personnel (ISP) to determine if resources (e.g., hardware, instrumentation, people) will be available during the anticipated dates. Once the TE is satisfied there are no obvious roadblocks then the TE will go through the process of creating a schedule request.

The TE then begins working with the ISP to identify which ground truth data elements the TE will need to evaluate the SUT. Ground truth data refers to measurements collected from properly calibrated instrumentation used as a means of providing a baseline “reality” vs. what the SUT “perceives” reality to be. The ISP will use that information to determine what instrumentation is required for the test, and where it should be placed to capture the required ground truth data (Figure 20). The TE documents, the instrumentation setup information, what we call in this thesis, the Instrumentation Configuration Plan.

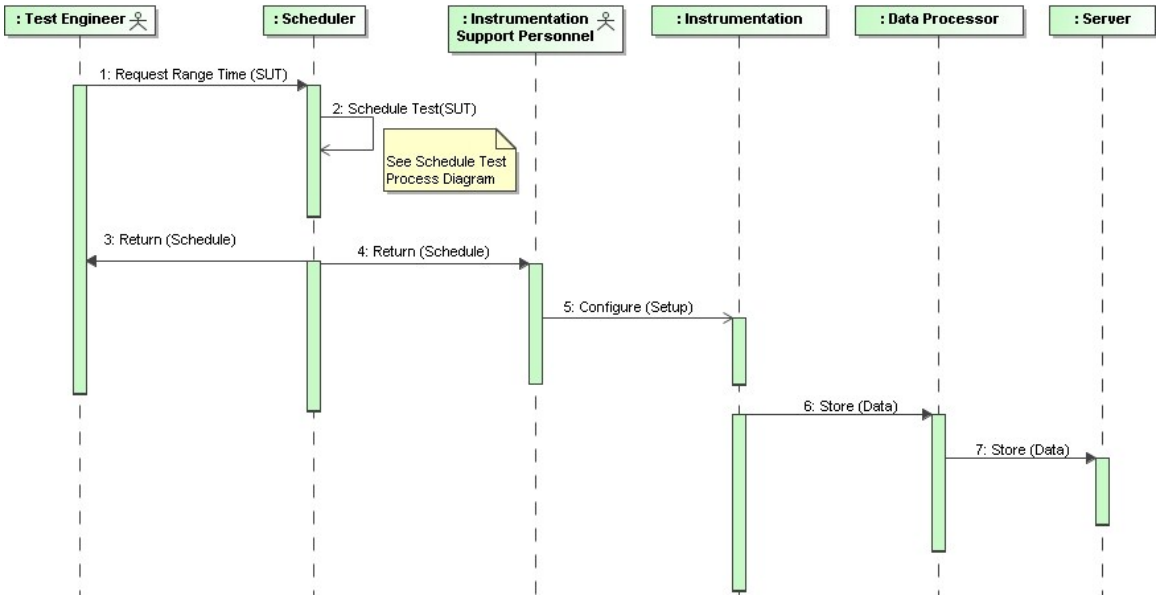

Figure 20. Pretest Setup Collaborations

b. Schedule Test Process

Currently, a standard tool does not exist within ATEC for scheduling range time or for identifying and resolving resource conflicts. Most test ranges have some type of home-grown application that performs parts of the scheduling deconfliction function. These tools merely enable more efficient communications between the parties that share resources and in most cases these collaborations will occur weeks prior to the SUT test date. If ranges do not have a tool to assist in their long-range and short-term planning and conflict resolution, range personnel utilize a manual process similar to the one depicted in Figure 21.

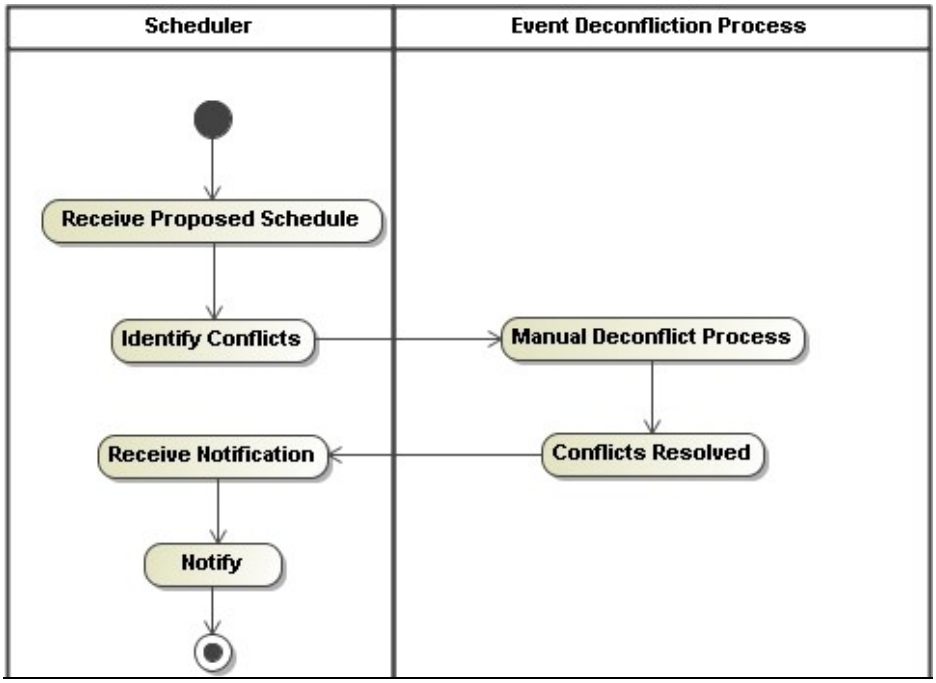

Figure 21. Schedule Test Process

At a range when a TE desires to put a test on the official authoritative schedule, several things must first occur. For example, a test location must be selected, safety fans must be established and evaluated, coordination must occur between this test and any conflicting tests, frequency authorizations (if needed) must be obtained, and spatial areas must be coordinated with any other scheduled tests, ranges, and potentially the Federal Aviation Administration (FAA) (via a Notice to Airmen (NOTAM) post.) This information is used by the home-grown scheduling tools or by individuals with grease or white boards to identify potential conflicts.

c. Event Deconfliction Process

LFT&E activities cover a wide range of operations, such as manned flight, unmanned flight, manned ground vehicles, unmanned ground vehicles, static ordnance tests, ordnance flight operations, climatic environmental tests, electromagnetic environment tests, road tests and operator training. Within a single TC, two or more of these activities regularly occur simultaneously and require coordination of shared resources such as radio frequencies, and spatial area (i.e., air, water, and ground space).

The deconfliction process typically takes place weeks prior to the requested test dates because the longer a TE waits to request time on the authoritative schedule the more likely the TE will have conflicts.

This scheduling event deconfliction process (Figure 22 and Figure 23) is an iterative process that repeats until all conflicts are either resolved or the schedule request is modified. Resolved means that either the conflicting SUT test date and time has been modified so that the conflicting test events can both occur, or that manual resolutions will need to occur prior to the SUT test occurring. Modifying the requested date and time is as simple as it sounds and will result in the TE going through the schedule test process and starting the event deconfliction process all over again because the change could result in new conflicts. Manually resolving resource conflicts can be time-consuming and error prone.

SUT test Alpha is scheduled for the same date and time as SUT test Beta and Alpha's safety fan barely overlaps with the safety fan for Beta causing a conflict. The responsible TEs could determine after consulting with the range safety officer and the standard operating procedures for both SUTs that both tests can stay on the schedule. However, a manual resolution is notated that Alpha must get positive confirmation via radio from the lead Beta POC that all Beta test personnel have exited the safety fan area prior to Alpha conducting its test.

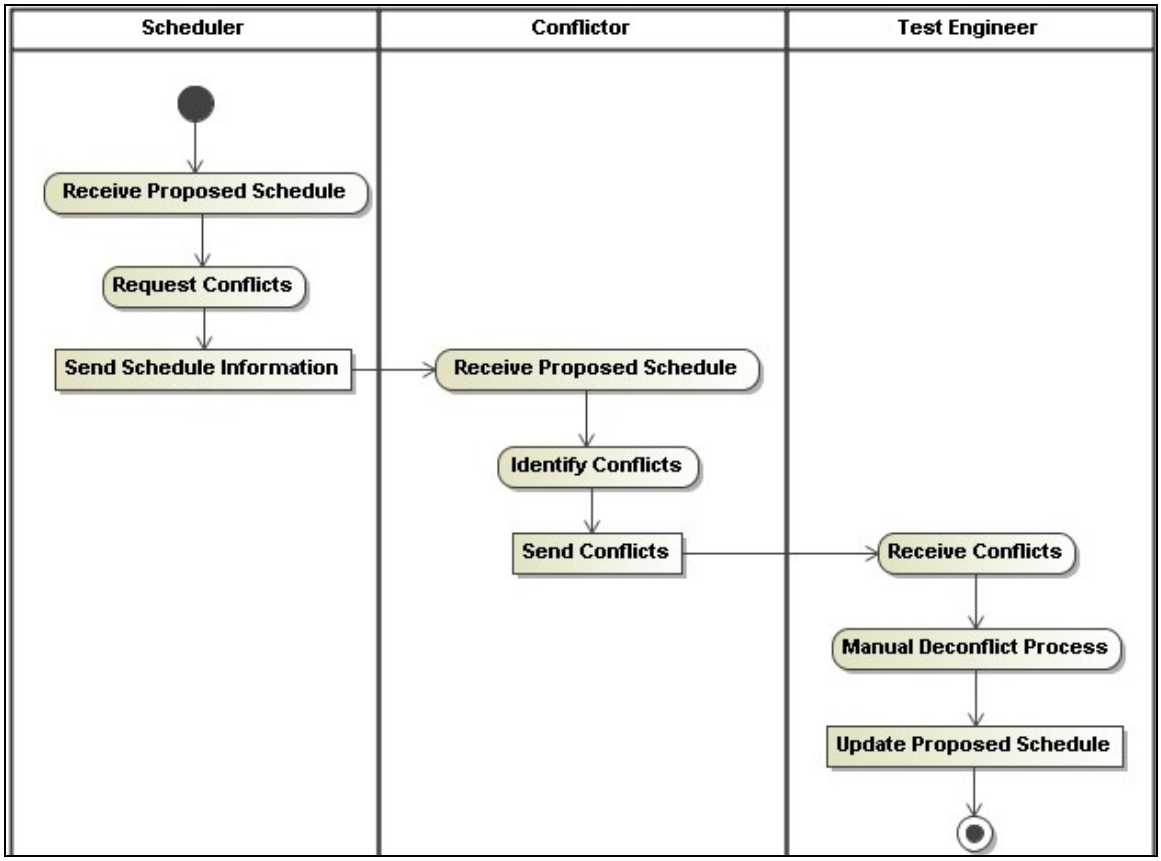

Figure 22. Event Deconfliction Process

Figure 23. Event Deconfliction Collaborations

3. Test Execution Process

After the TE has successfully planned for and scheduled the test event, the TC range hosts each of the competing contractors and conducts testing on each SUT individually. Everything up until this point has been equivalent to a dress rehearsal for a play with each actor rehearsing his or her lines and movements. During the test execution (Figure 24), the Instrumentation Configuration Plan is executed, all test setup information is documented for archival purposes (in case the test needs to be performed again in the future), the test plan is executed, the test occurs (e.g., missile is fired, vehicle is shaken, aircraft is flown, explosive is detonated), and ground truth data is collected (Figure 25).

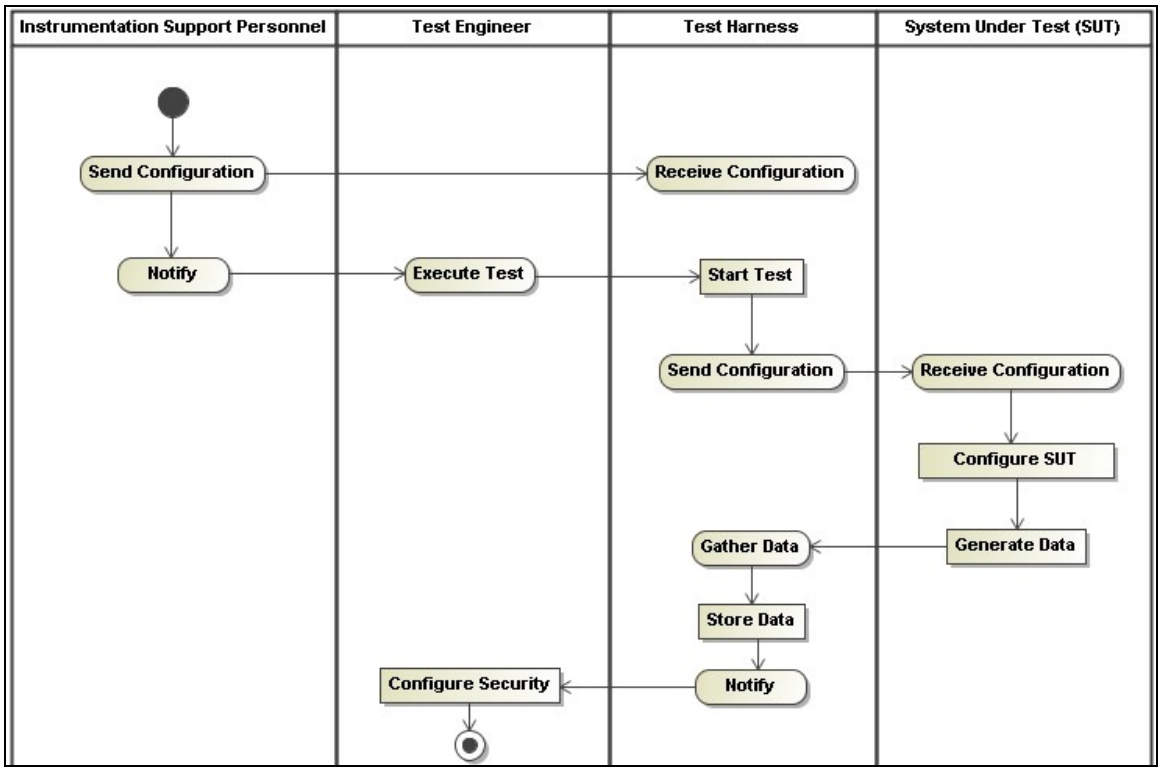

Figure 24. Test Execution Process

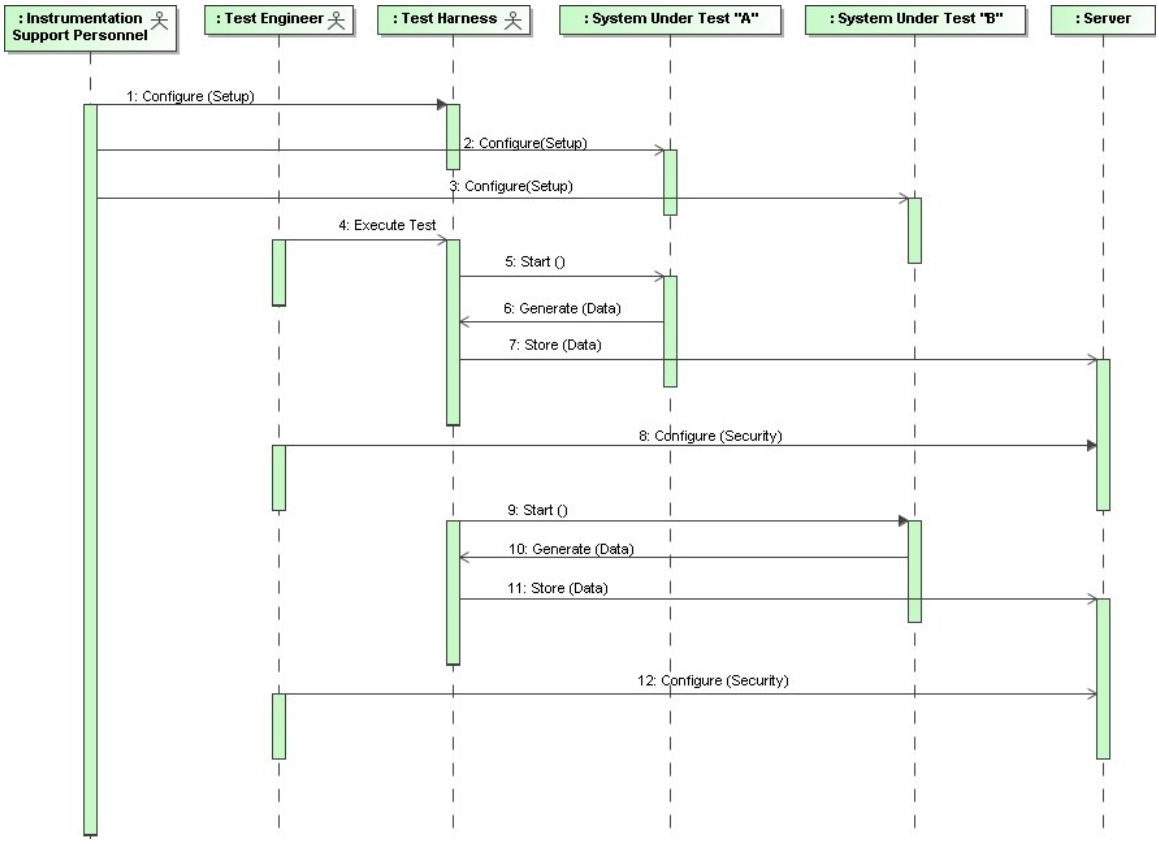

Figure 25. Test Execution Collaborations

4. Post-test Data Analysis Process

During testing, a large amount of raw data and ground truth data is generated. This data must be collected, stored, and secured for analysis and reduction. At the conclusion of the test, the TE is responsible for coordinating with all involved Instrumentation Support Personnel to gather collected raw test data and sensor ground truth data (Figure 26). The ISP will collect the data from the various instruments, sensors, and perhaps even the SUT itself. Typically, this raw data is stored on a local server and can consist of everything from small binary files, high-resolution photo and high-speed video files, to high-fidelity Time Space and Position Information (TSPI) data. The TE will then be notified by some mechanism, typically verbal or e-mail, that all information has been collected and stored at the central range location.

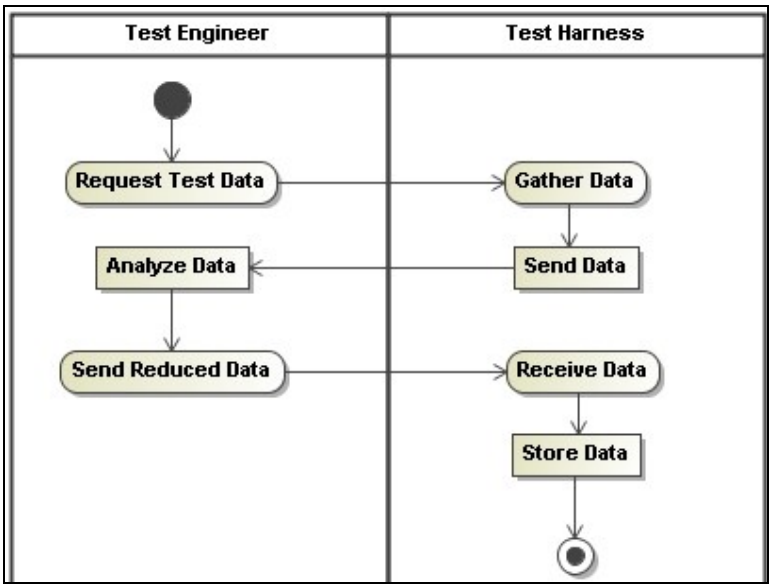

Figure 26. Post-test Data Analysis Process

The TE is responsible for setting permissions on these files, which is paramount as at all times the competing contractors should not be allowed to see any information regarding their competition or even know that a test has been conducted on their product. For example, if contractor “Alpha” were to inadvertently gain access to information regarding competing contractor “Beta” then this could give “Alpha” an unfair advantage. Even knowing the number of times “Beta” has been at a test range, the number of flights performed by “Beta,” or even the fact that “Beta” has flights on a test range’s upcoming schedule could potentially be used by “Alpha” to determine if “Beta” is having problems in their development. If “Beta” ever discovered that “Alpha” had access to such information, and “Alpha” won the eventual contract award, it could lead to a costly contract protest.

After the data has been properly secured on the server, the TE then begins the process of verifying that there were no anomalies in the collected ground truth data and begins reducing the collected test dataset to contain only the information pertinent to the test objectives (Figure 27). This reduced dataset is typically stored both on the server and also temporarily stored on the TE’s local machine. Ultimately, all of the reduced data is used by the TE to generate the final TR.

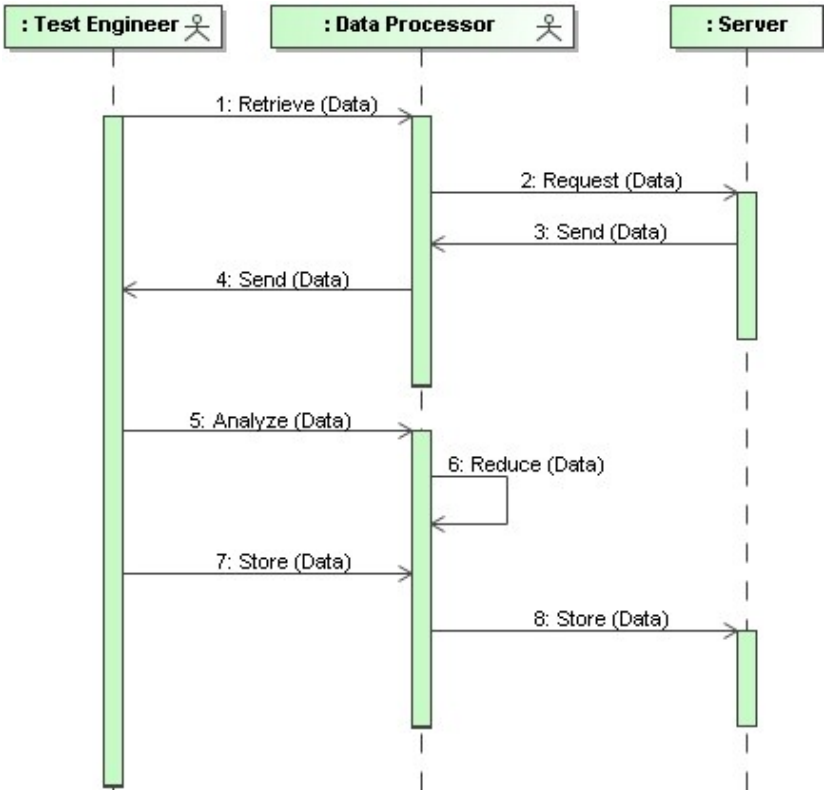

Figure 27. Post-test Data Analysis Collaborations

a. Test Report Generation Process

Everything described within Chapter III.C, from the initial Program Management through the various steps of Pretest Planning, Scheduling, and Deconfliction to Conducting the Test, has been leading up to the generation of the final TR. The process that started in Chapter III.C.1 culminates with the delivery of the final TR to the PM (Figure 28).

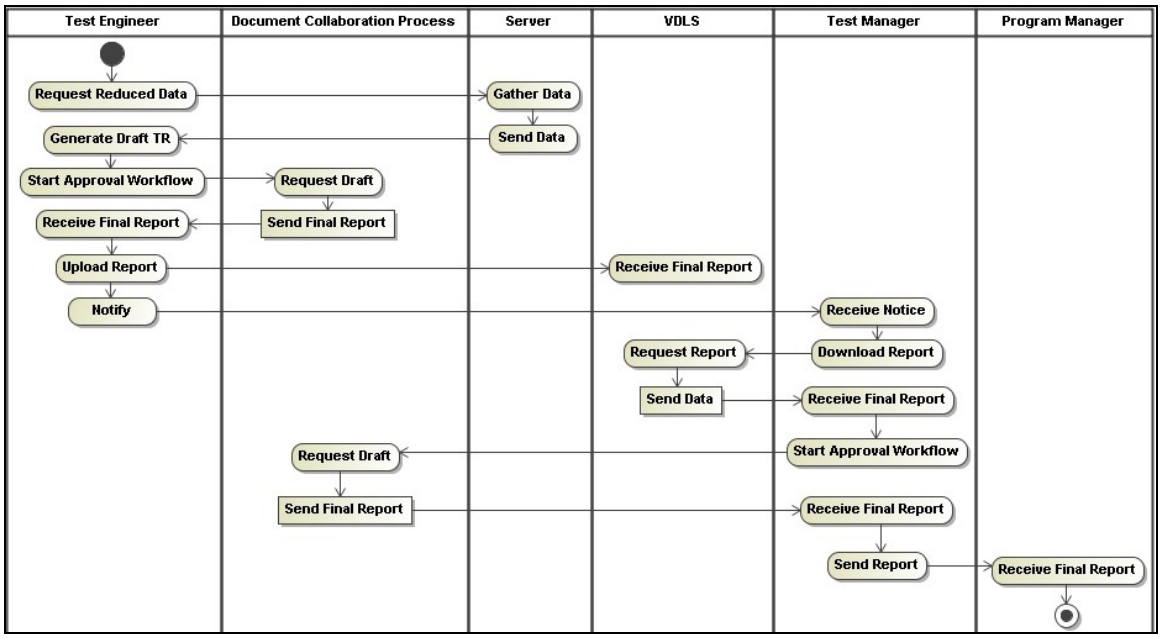

Figure 28. Test Report Generation Process

Test Reports (TR) document the results of a test and usually recommend a course of action based on those results. The TR addresses test results, including test conducted, data collected, the data reduction and analysis process, and conclusions to be drawn from the test data. Overall, it provides data on the T&E activity completed during the engineering and development phase of a program to verify that the hardware and software design meets the specified requirements.

DoD Instruction 5000.02 requires the PM of a program designated for the Office of the Secretary of Defense (OSD) T&E oversight to provide reports of results, conclusions, and recommendations from Developmental Test and Evaluation (DT&E), OT&E, and LFT&E to the Director, Operational Test and Evaluation (DOT&E) and Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) ("DoD Instruction 5000.02, Operation of the Defense Acquisition System," 2010). For those reports supporting a decision point, the report will identify the strengths and weaknesses in meeting the warfighters, documented requirements based on developmental evaluations. The content of the report is the impartial evaluation from the DT&E Responsible Test Organization (RTO) of a system's military utility and

capabilities against warfighter requirements. The DT&E report will provide a historical record of the final T&E results for the system. In addition, the TR should include the RTO's assessment of a system's military utility, capabilities and limitations; document the test techniques, procedures, and data analysis; and provide data for operating and employment and maintenance manuals for the system. At the conclusion of LFT&E, the DOT&E prepares an independent assessment report that describes the results of the survivability or lethality LFT&E, and assesses whether the LFT&E was adequate to provide information to decison makers on potential user casualties and system vulnerabilities or lethality is based on testing under realistic conditions, consideration of the validated statement of desired operational capabilities, the expected threat, and susceptibility to attack ("Defense Acquisition Guidebook Ch. 9.7. Test and Evaluation Reporting of Results," 2010).

Figure 29 shows the typical collaborations between the TE and the TM prior to a final TR being delivered to a PM. After the TE has reviewed and reduced all data collected during the test, then the TE prepares a draft TE TR. Prior to the draft TE TR being finalized, it must go through an iterative document collaboration and review processes with the TE Supervisor after which it is delivered to the TD where it is combined with any other TE TRs that were part of the same main test for the TC. This combined report, after going through an iterative document collaboration and review process discussed in the next section, will become the final TC TR and will be uploaded to the VDLS location that was previously created.

The internal TC portion of the process described above can take ninety plus days to complete and during this time it is highly likely that while collaborating on the final TR the TE, supervisor, or TD will be sent on a temporary duty assignment (TDY). This leads to configuration control issues as the person going TDY must download a copy of the current version of the document from the server, make changes while TDY, and upon returning must manually deconflict any changes that were made to the document by the other reviewers.

After the final TC TR has been uploaded to VDLS, the TM will then be notified that the final TC TR has been uploaded to VDLS. The TM will then collect the final TC TRs from all TCs that were involved in the overall test. The TM will then go through an iterative document collaboration and review process to create the final TR. This final TR is the report described in DoD instruction 5000.02 and will be sent to the PM.

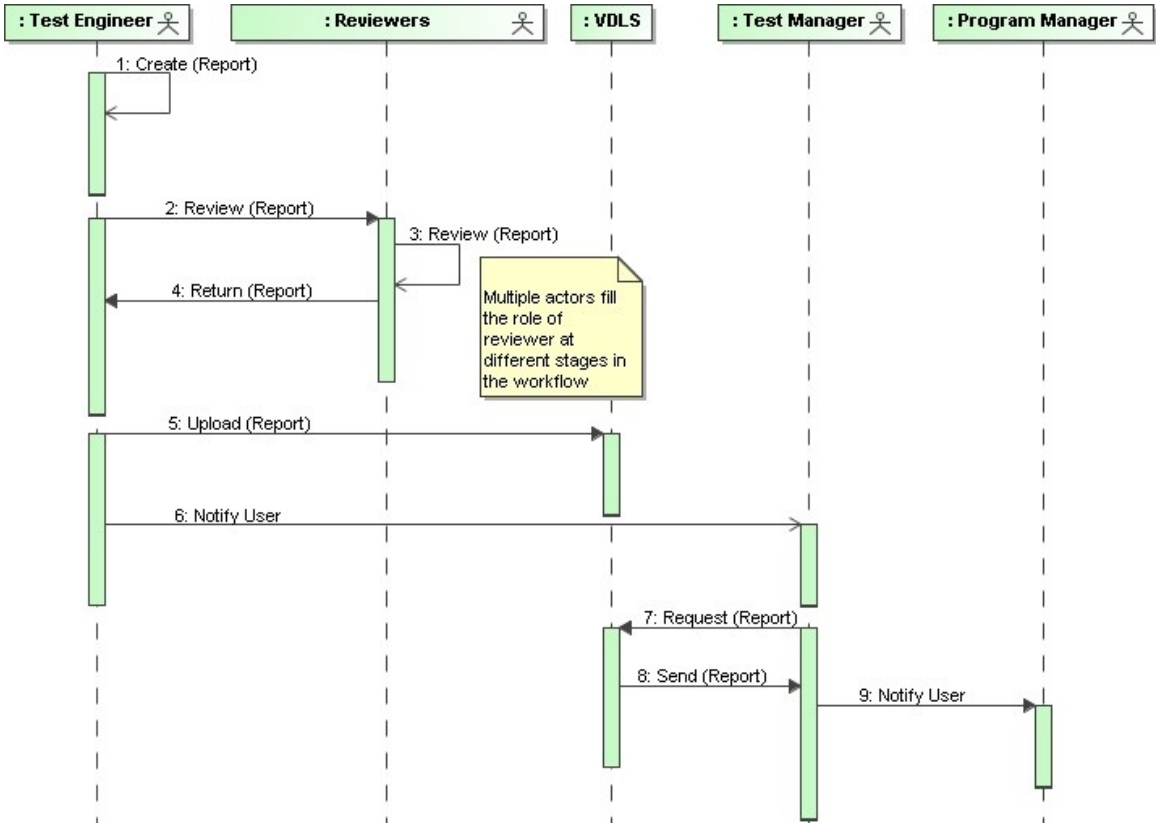

Figure 29. Test Report Generation Collaborations

5. Document Collaboration Process

When a document enters the document collaboration process, as illustrated in Figure 30, it goes through the same abstract process regardless of where the document originates from or who it will ultimately be delivered too and involves contributors and reviews. The contributors send the draft document to the reviewers who review the

document and either approve it or don't approve it. If the draft is approved, then the draft's nomenclature is changed from draft to final. If the draft is not approved, then the reviewers will send comments back to the contributors. The contributors will then make the requested changes and resubmit a new draft starting the entire process over again.

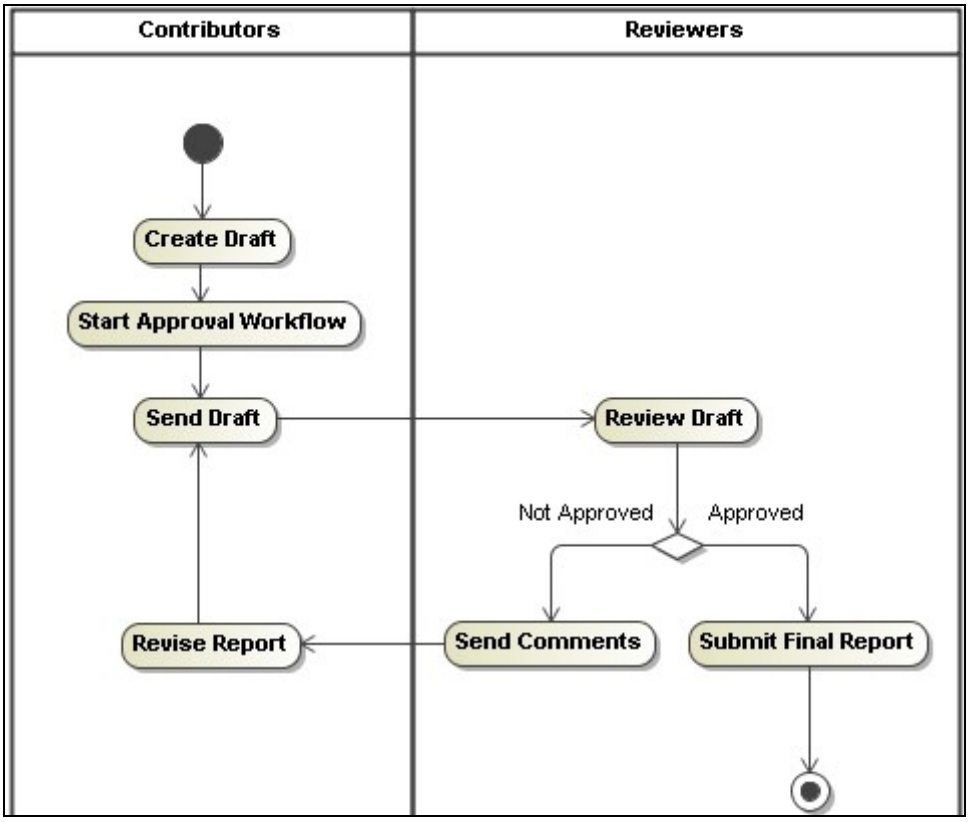

Figure 30. Document Collaboration Process

D. USE CASE ANALYSIS SUMMARY

Figure 31 presents a Use Case model for the typical T&E mission thread described in Chapter III.C, which is made up of nine use cases described in Tables 1–9 in this section.

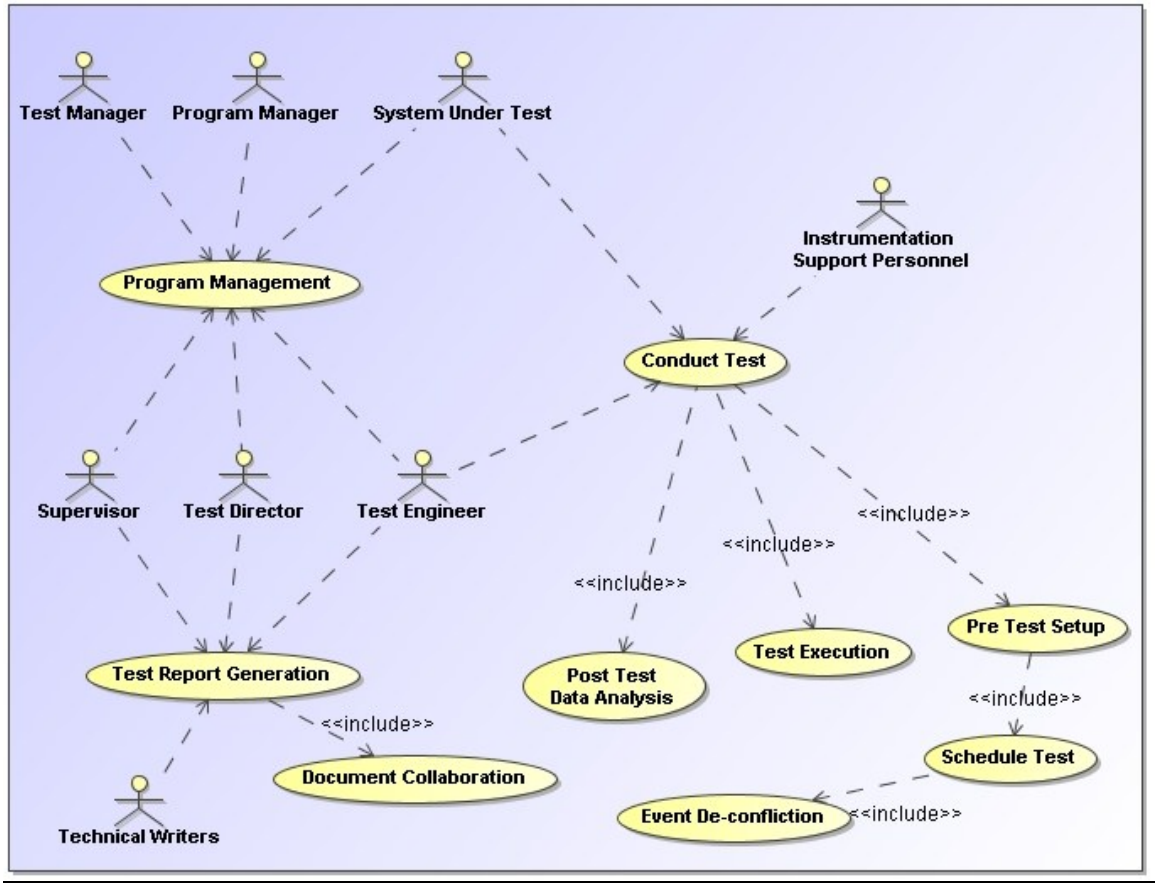

Figure 31. Mission Thread Scenario

UC1	Program Management
Description	A Program Manager (PM) requests a new LFT&E test.
Desired outcome	A test program is initiated with the test requirements flowing from the PM to the appropriate TC and eventually to the appropriate TE for the test.
Assumptions	None
Actors	• Program Manager (PM) • Supervisor • System Under Test (SUT) • Test Center (TC) • Test Director (TD) • Test Engineer (TE)

	• Test Manager (TM)	
Dependencies	None	
Process flow	Step description	Artifact
	1. PM submits a Request for Test Services (RFTS)	RFTS created
	2. ATEC Initiates the request, creating an ADSS Effort Shell (Effort)	ADSS Effort Shell created
	3. ATEC creates Microsoft Project Plan in PMES	Project Plan created in PMES
	4. TM selects Test Center (TC)	
	5. TM activates Effort	Effort activated within ADSS
	6. TM forward Effort to TC	
	7. TC selects TD	ADSS TC POC field updated
	8. TD gathers requirements	
	9. TD generates Test Plan	Initial Test Plan created ADSS Milestones updated VDLS Folder Structure created
	10. TD selects Division	
	11. Division Supervisor selects TE	
Deliverables	• ADSS Effort • Initial Test Plan • Project Plan • Test Requirements	
Additional information	None	

Table 1. Use Case 1: Program Management

UC2	Conduct Test	
Description	Using the requirements and initial test plan a test will be conducted. This will require pretest planning, scheduling coordination, event deconfliction, test execution, and post test data analysis.	
Desired outcome	To successfully conduct the test, obtain the data elements that will allow the TE to properly evaluate the SUT, and reduce the data in preparation for the generation of a formal Test Report.	
Assumptions	• Funding has arrived, safety fans have been created, and environmental impact concerns have been addressed. • No external issues exist to prevent test from occurring. • System Under Test (SUT) is onsite at the Test Center (TC)	
Actors	• Instrumentation Support Personnel (ISP) • Test Engineer (TE) • System Under Test (SUT)	
Use cases involved	• Post-test Data Analysis UC7 • Pretest Setup UC3 • Test Execution UC6	
Dependencies	• Initial Test Plan • Test Requirements	
Process flow	Step description	Artifact
	1. Pretest setup	Finalized test plan
	2. Schedule test	Test on authoritative schedule
	3. Test execution	Raw test data collected
	4. Post test data analysis	Test data reduced
Deliverables	• Finalized Test Plan • Scheduled Test • Raw Test Data • Reduced Test Data	
Additional information	None	

Table 2. Use Case 2: Conduct Test

UC3	Pretest Setup	
Description	Prior to test execution a great deal of upfront planning must occur. The test plan must be finalized, instrumentation must be configured, schedules must be coordinated, the test must be added to the authoritative schedule, and test setup information must be fully documented.	
Desired outcome	To perform the proper upfront planning and coordination for the test execution to be repeatable and be executed with as few oversights as possible.	
Assumptions	• Test Plan has been finalized.	
Actors	• Instrumentation Support Personnel (ISP) • Schedule Test Process • Scheduler • Test Engineer (TE)	
Use cases involved	• Schedule Test Process UC4	
Dependencies	• Initial Test Plan • Test Requirements	
Process flow	Step description	Artifact
	1. Test Engineer requests range time*	Schedule Request
	2. Test scheduled by Schedule Test Process* (UC4)	Authoritative Schedule for SUT
	3. Notify ISP and TE	
	4. ISP configures instrumentation	Instrumentation Configuration Plan
	5. Store Configuration Plan	
Deliverables	• Schedule Request • Instrumentation Configuration Plan • Authoritative Schedule for SUT	
Additional information	* Step 1 and 2 will continue will continue until the requested schedule successfully goes through the Schedule Test Process (UC4).	

Table 3. Use Case 3: Pretest Setup

UC4	Schedule Test	
Description	Put a test on the authoritative range schedule.	
Desired outcome	Successfully schedule range time and all required resources needed to support a test.	
Assumptions	• All required resources are known and identified prior to scheduling test	
Actors	• Event De-confliction Process • Scheduler • Test Engineer	
Use cases involved	• Event De-confliction (UC5)	
Dependencies	• Final Test Plan	
Process flow	Step description	Artifact
	1. * Schedule Request received from Test Engineer	Proposed Request
	2. * Conflicts identified by Event De-confliction process (UC5)	
	3. Conflicts resolved	Test Engineer notified Test added to Authoritative Schedule
Deliverables	• Authoritative Schedule for SUT	
Additional information	* Step 1 and 2 will continue will continue until all conflicts are addressed.	

Table 4. Use Case 4: Schedule Test

UC5	Event De-confliction	
Description	Identify and resolve potential scheduling conflicts prior to test events being added to the authoritative schedule.	
Desired outcome	To have a fully deconflicted schedule, so there is not a schedule delay due to lack of prior coordination between test programs.	
Assumptions	None	
Actors	• Authoritative Schedule Information • Conflictor • Conflictor Data • Scheduler • Test Engineer	
Use cases involved	• Schedule Test (UC4)	
Dependencies	• Proposed schedule	
Process flow	Step description	Artifact
	1. Receive proposed schedule	
	2. Request scheduled events	
	3. Identify conflicts	List of conflicts
	4. Send conflict list to user	User Notified
Deliverables	• List of conflicts	
Additional information	If no conflicts are present then the user is notified that no conflicts were found. This process will repeat with UC4 until all conflicts are addressed.	

Table 5. Use Case 5: Event De-confliction

UC6	Test Execution	
Description	LFT&E test occurs and data is collected.	
Desired outcome	The test plan is executed with no problems with data being successfully collected, stored, and secured for later reduction by the Test Engineer (TE).	
Assumptions	• All conflicts have been handled and any manual resolutions have occurred. • All instrumentation has been configured properly • Competing contractors are not present	
Actors	• Instrumentation Support Personnel (ISP) • Server • System Under Test (SUT) • Test Engineer (TE) • Test Harness	
Use cases involved	None	
Dependencies	• Test is on authoritative schedule • Instrumentation Configuration Plan is complete and available • Final Test Plan is complete and available	
Process flow	Step description	Artifact
	1. Instrumentation is configured	
	2. Test is executed	Raw Data is generated
	3. Raw data is collected and stored on the server	User notified of location
	4. TE configures security on raw data	Properly Secured Raw Data
Deliverables	• Raw Test Data	
Additional information	None	

Table 6. Use Case 6: Test Execution

UC7	Post-test Data Analysis	
Description	Raw data is reduced by the Test Engineer (TE) into a useable form.	
Desired outcome	While reducing the raw data the TE begins evaluation of the System Under Test (SUT) and has enough information to generate a formal Test Report (TR).	
Assumptions	None	
Actors	• Data Processor • Test Engineer (TE) • Server	
Use cases involved	None	
Dependencies	• Raw Test Data	
Process flow	Step description	Artifact
	1. Retrieve raw data	
	2. Analyze raw data	Reduced Data
	3. Store reduced data	
Deliverables	• Reduced test data	
Additional information	None	

Table 7. Use Case 7: Post-test Data Analysis

UC8	Test Report Generation
Description	Compilation of a Final Test Report based on the Test Engineer's analysis of the reduced data.
Desired outcome	A fully documented Final Test Report that is delivered to the Program Manager and is used by senior leadership to evaluate the effectiveness of the System Under Test (SUT).
Assumptions	None
Actors	• Program Manager (PM) • Reviewers

	• Server • Test Engineer (TE) • VDLS	
Use cases involved	• Document Collaboration (UC9)	
Dependencies	• Reduced Test Data	
Process flow	Step description	Artifact
	1. Using reduced test data create draft Test Center (TC) Test Report (TR)	Draft Test Center Test Report
	2. Begin Draft Approval Workflow (UC9)	
	3. Final TC TR Approved	Final Test Center Test Report
	4. Upload Final TC TR to VDLS	VDLS Populated
	5. Notify Test Manager (TM)	User Notified
	6. Collect all final TC TRs from VDLS	
	7. Create draft Final TR	Draft Final Test Report
	8. Begin Draft Approval Workflow (Document Collaboration UC9)	
	9. Final TR Approved	Final Test Report
	10. Notify Program Manager (PM)	User Notified
Deliverables	• Draft Test Report • Final Test Report • VDLS Populated	
Additional information	None	

Table 8. Use Case 8: Test Report Generation

UC9	Document Collaboration	
Description	Transformation of the draft Test Report into a Final Test Report through an approval workflow with all pertinent parties.	
Desired outcome	To have an approved Final Test Report that all pertinent parties have been able to review prior to release.	
Assumptions	None	
Actors	• Contributors • Reviewers	
Use cases involved	None	
Dependencies	• Draft Test Report	
Process flow	Step description	Artifact
	1. Draft Report e-mailed to reviewers	
	2. Draft Report Reviewed	Comments
	3. Draft Report Approved	Final Test Report
Deliverables	• Final Test Report	
Additional information	Steps 1 and 2 are continued until all comments are addressed and all reviewers approve the draft.	

Table 9. Use Case 9: Document Collaboration

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CLOUD BASED T&E PROCESS

A. INTRODUCTION

Currently within ATEC, a place does not exist where a PM can go and obtain all of the information related to an acquisition program, regardless of how many TCs that program crosses, that is the "one stop shop", or integrated working environment (IWE), does not exist. Instead, the PM must rely on contacting individuals familiar with the program to obtain the information. In this chapter, we explore how cloud computing could be used to improve upon current workflow processes utilized by PMs within ATEC. Currently PMs must first contact the TM, who then contacts the TD, who then contacts the TE, who then tells the TD when the test is scheduled for range time (Figure 32).

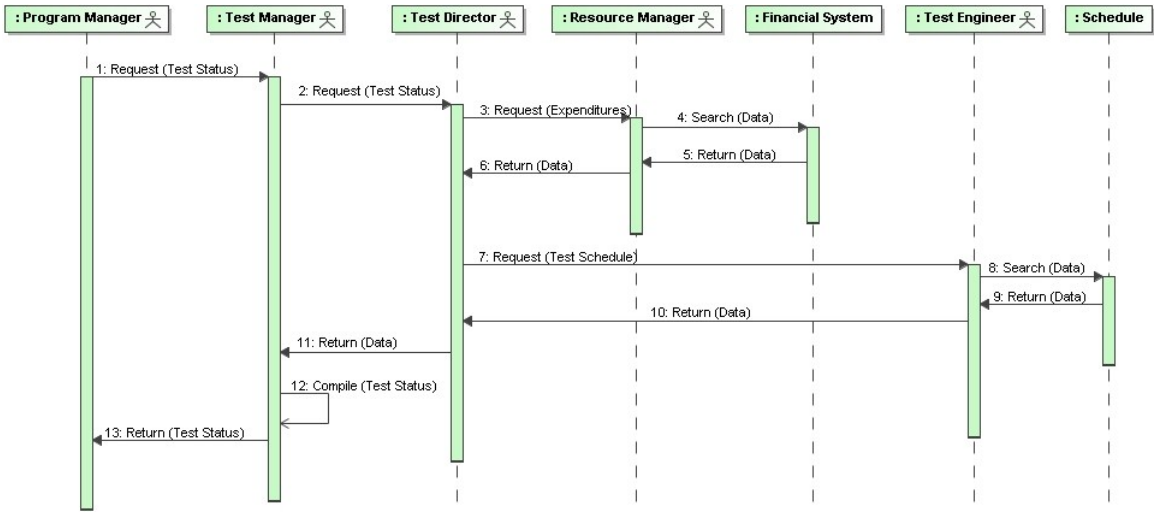

Figure 32. Program Management Data Call Collaboration As-Is

This information is then relayed back to the requestor in a serial manner, with additional delay introduced whenever someone in the chain of communication is unavailable. Even though this scheduling information, in most cases, is available via scheduling tools at the TC level, the PM does not have access to the locally stored

scheduling data. The same scenario exists if the PM wants to know the current financial status for the test. While the PM can see the high-level information within SOMARDS, the information available may not be current due to the posting cycles at the TC. In other words storing the data locally, that is on the workstation, is an impediment to information sharing within ATEC and with ATEC's stakeholders.

Given that the information available at the TE level is the most up-to-date information about the test, that data should be available to all parties with a need to know. This combined with ready access to the financial information and other programmatic information would provide senior leadership with the situational awareness about their acquisition programs and those across the entire command. Ideally, the framework for the IWE would be created when the RFTS is submitted. From that moment on, all information related to that program would be accessible from the IWE, with all of the data along with the applications that operate on the data residing in the ATEC cloud. Figure 33 depicts the cloud-enabled program management data-call process.

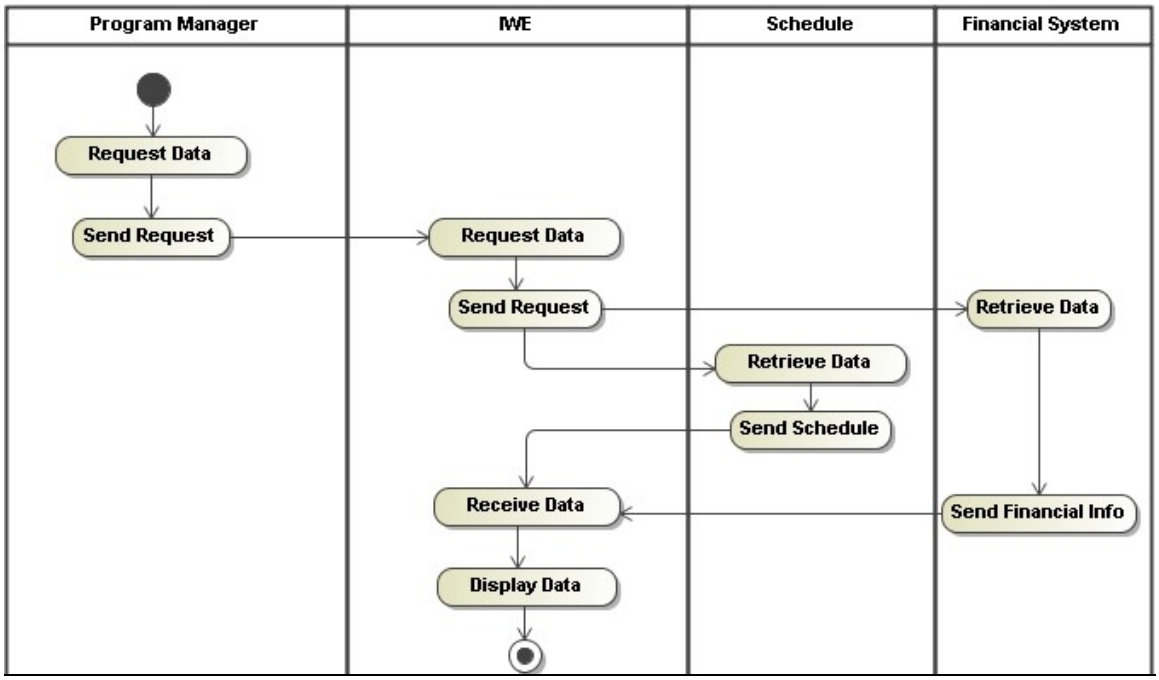

Figure 33. Program Management Data Call Process in the Cloud

All this data would not have to physically reside within the cloud-based IWE. Initially, the information could reside in legacy systems and be consumed through Web services or reside in a cloud APC (Figure 34). The IWE would be merely a front end to a search-and-index tool with interfaces to raw unstructured data (e.g., cloud APC file system, existing TC data center, documents, raw test data, video, images), structured data (e.g., relational databases, spreadsheet, xml), and legacy systems (e.g., scheduling tools, financial tools).

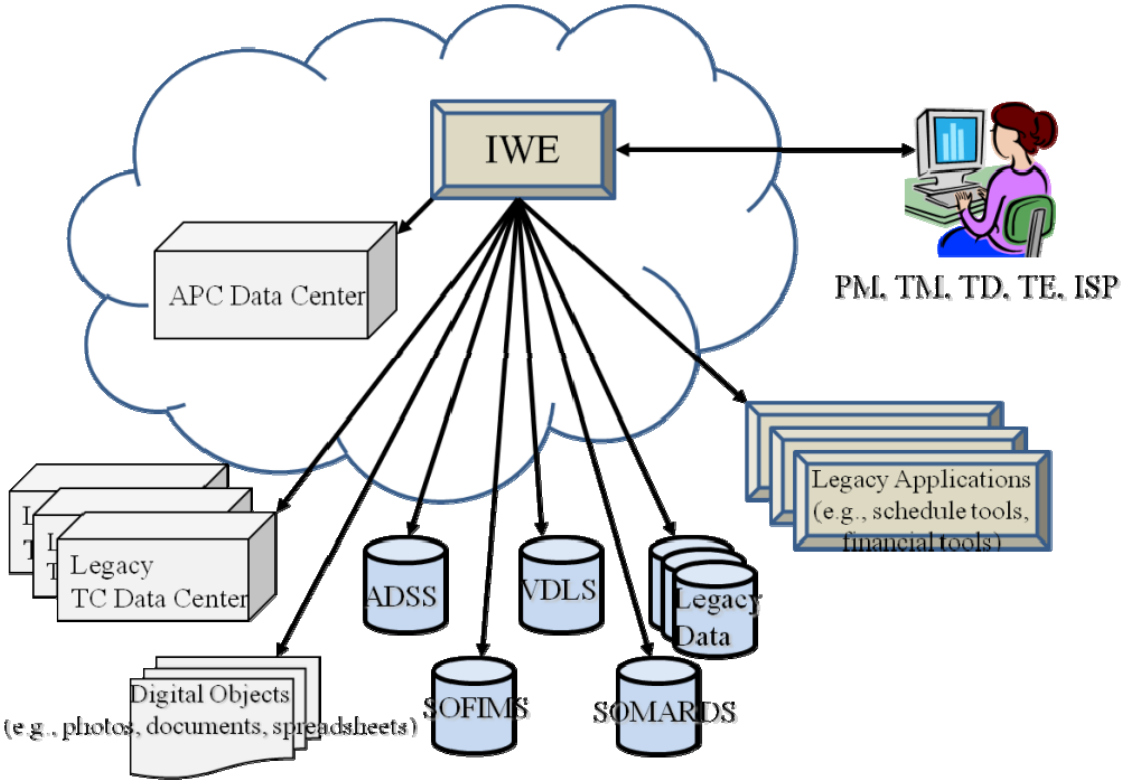

Figure 34. Cloud T&E Architecture

Does this solution require cloud computing? No, it could be done today through extremely tight coupling of existing systems. However, that rigid coupling is difficult to achieve across various functional divisions within one TC much less across all of ATEC. This has been one of the stumbling blocks that have prevented a true “soup-to-nuts” enterprise solution from being deployed. Within a cloud environment though, this could

be accomplished with less rigidity through the use of SaaS and the migration of data into the cloud.

B. CLOUD BASED T&E MISSION THREAD

The Use Cases from Chapter III, which have the potential to change the most within a cloud environment, will be expanded upon in the following sections with an overview of potential new functionality described, along with the mission thread described within Chapter III.C.

Whether explicitly mentioned or not, at every level of the processes described below role-based access controls (RBAC) are needed to protect sensitive data. People within the enterprise can be assigned to roles with permissions associated with the roles. The details for applying RBAC in the cloud are being investigated within the cloud-security communities. It is worth mentioning that at the TD and TE level there will potentially be concerns about the PM having the level of detail described below: such access could be viewed as opening the door to micromanagement. The detailed design of such security access controls and the industrial organization psychology and management aspects of sharing data enterprise-wide is outside the scope of this thesis.

1. Program Management in the Cloud

While moving data and applications to the cloud would provide additional functionality through the mash-up of previously disconnected datasets, and non-interoperable applications for manipulating the data, the process would not change dramatically. The process would still begin with a request for test services that would automatically start a workflow to identify a TM and create a cost estimate. All of the current ties to ADSS and VDLS would either still exist as-is or would be simplified through the replacement of VDLS with the IWE (Figure 35). In essence, VDLS and ADSS would be just another data source for the IWE to pull information from.

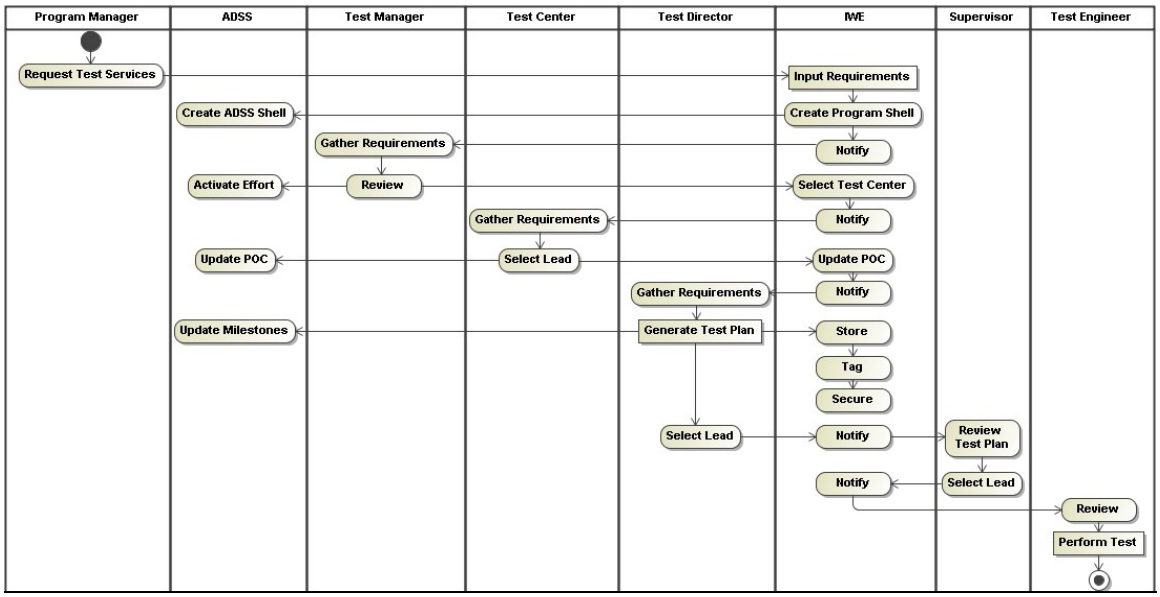

Figure 35. Program Management Process in the Cloud

The overall collaborations within the program management process would be essentially the same as the current system. The only notable difference would be the replacement of VDLS with the IWE and the replacement of all current e-mail communications with collaboration through the IWE (Figure 36).

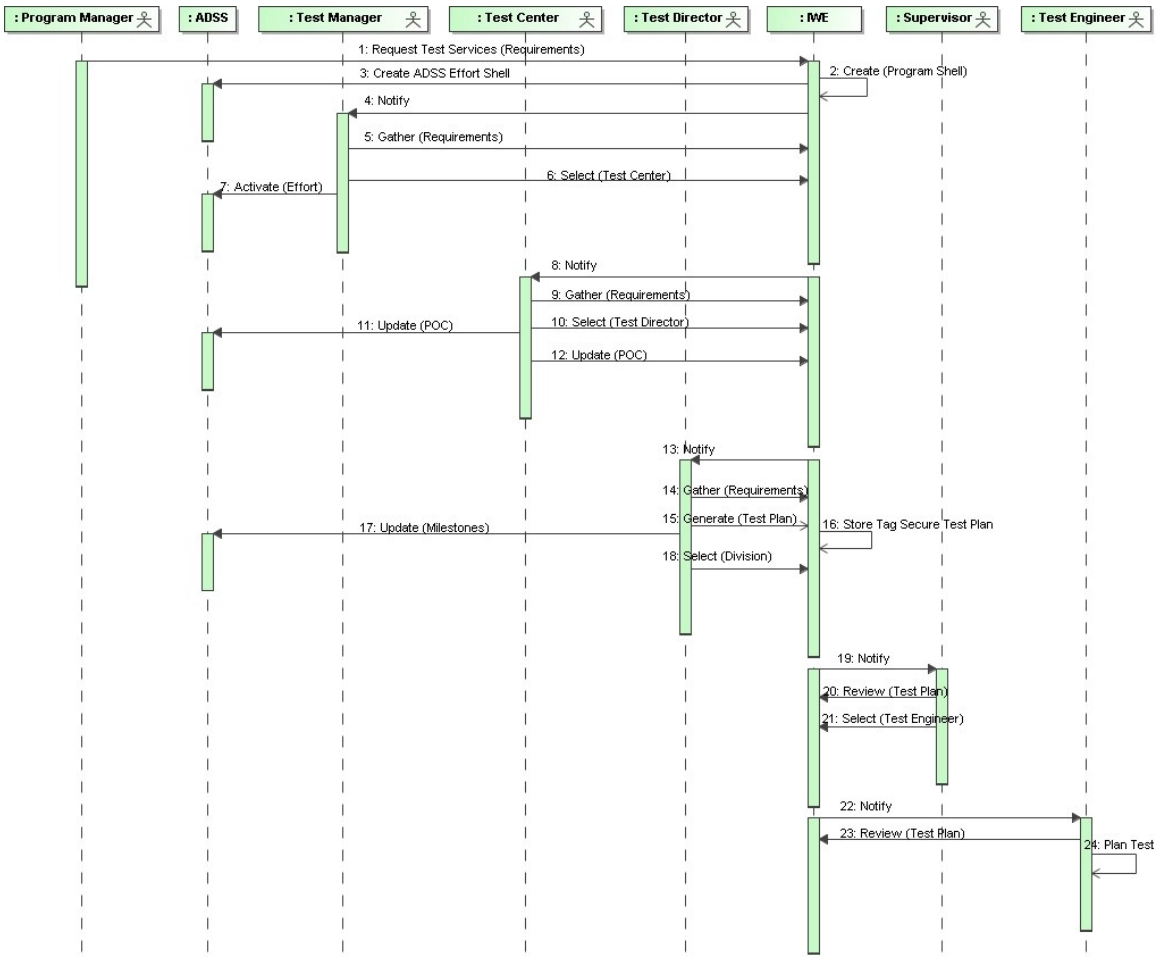

Figure 36. Program Management Collaborations in the Cloud

Where the current process and the cloud process would differ the most is within the monitoring, reporting, and control aspect of program management, and the ability of the cloud solution to provide a consistent up-to-date view of the data across the enterprise. The current method for monitoring, reporting, and controlling a program relies on a primarily manual process. In contrast, a cloud-based system could permit a certain amount of automation of the information processing and sharing functions, essentially eliminating the middleman, or put another way, the human-in-the-loop for updating the information displayed by the IWE, as shown in Figure 37.

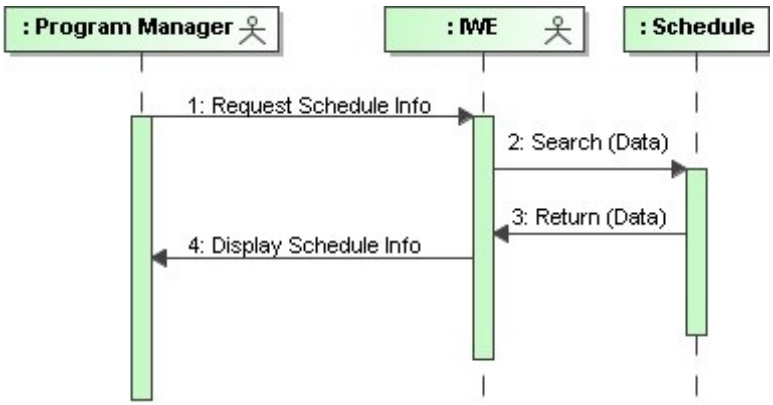

Figure 37. Program Management Data Call Collaboration in the Cloud

2. Conduct Test Process

Just as in the process described in Chapter III, the conduct test process within the cloud revolves heavily around the TE conducting and managing the day-to-day status for each test. Each selected TE is responsible for either performing or coordinating all aspects of their portion of the test plan, covering everything from pretest test planning, test execution, post-test analysis and data verification, to collaboratively writing the final test report. Within a cloud environment, the main items that will change will be the data storage location and the test report process.

a. Pretest Setup Process

Since conducting a test is potentially a destructive and costly process, coordination is needed among those people involved in planning for tests. That way the test does not have to be repeated at a later date due to poor planning. This coordination occurs during the pretest planning and setup process. Currently, the pretest planning and setup process relies heavily on informal interactions between the TE and other TEs in addition to range personnel. Most of these interactions occur in verbal communications and as such are not being captured in a manner that is searchable or retrievable at a later date. When personnel leave the organization, their knowledge of the programs and workflow processes disappears with them. However, if the pretest planning and setup process took advantage of cloud-based social media tools then these informal

collaborations could be captured where they could be tagged, indexed, searched, and archived (Figure 38). Examples of such tools include IBM's LotusLive, Salesforce Chatter, and Facebook.

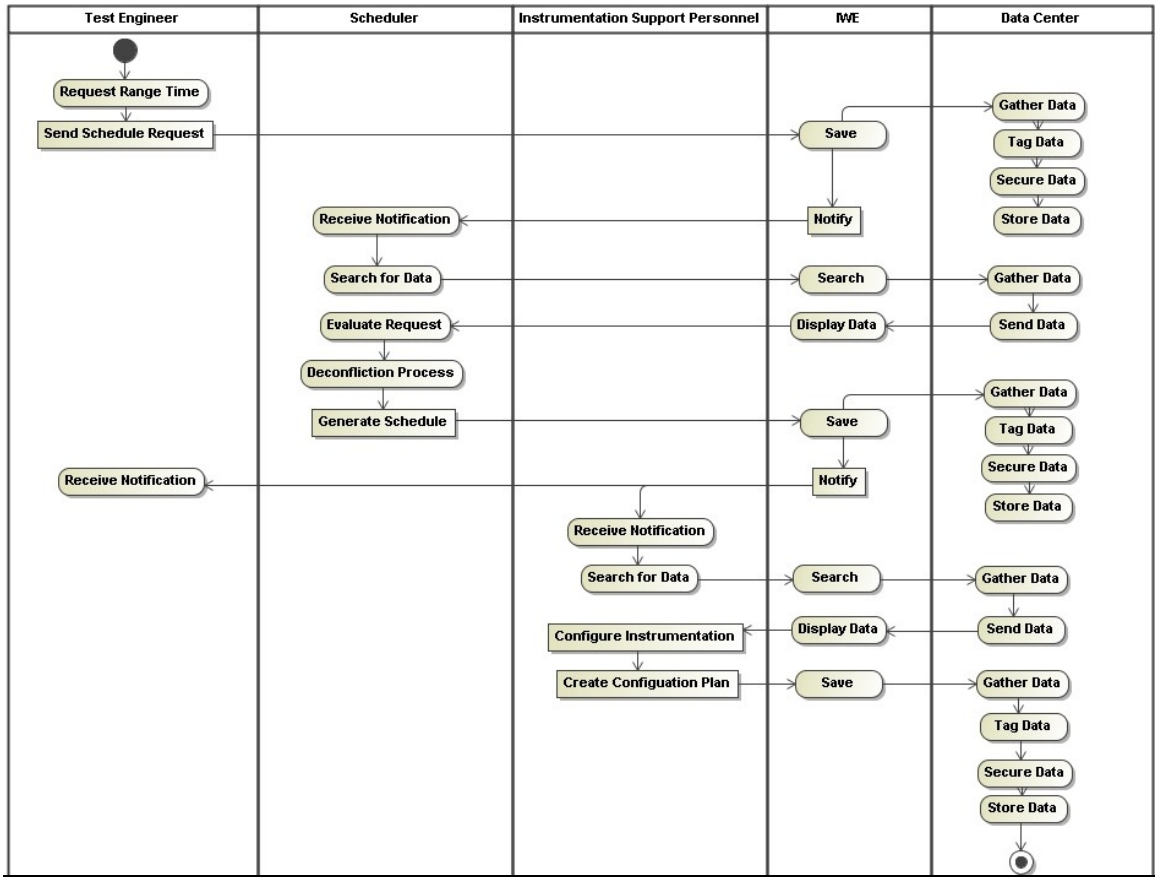

Figure 38. Pretest Setup Process

Having the ability to search through these interactions would help DoD amass the large amount of undocumented corporate knowledge employees currently posses in their heads into documented and searchable data. The IWE could provide the nexus for the social media tools that would make this possible. Tools, such as online document editors, instant messaging, threaded message boards, wikis, blogs, tags, status updates, ratings, polls, news, hot topics, tasks, RSS feeds, tweets, and so on would all provide for a rich collaborative environment.

The TE will continue to work with the ISP to identify which ground truth data elements the TE will need to evaluate the SUT. The ISP will use that information to determine what instrumentation is required for the test, and where it should be placed to capture the required ground truth data (Figure 39). However, within a cloud environment this collaboration could occur within the tools in the IWE, which would provide all of the benefits that were previously mentioned. The Instrumentation Configuration Plan could be created and tagged within the IWE. The plan could theoretically be created on a smartphone or tablet PC and uploaded to the IWE directly from the field through for instance a wi-fi or 3G connection.

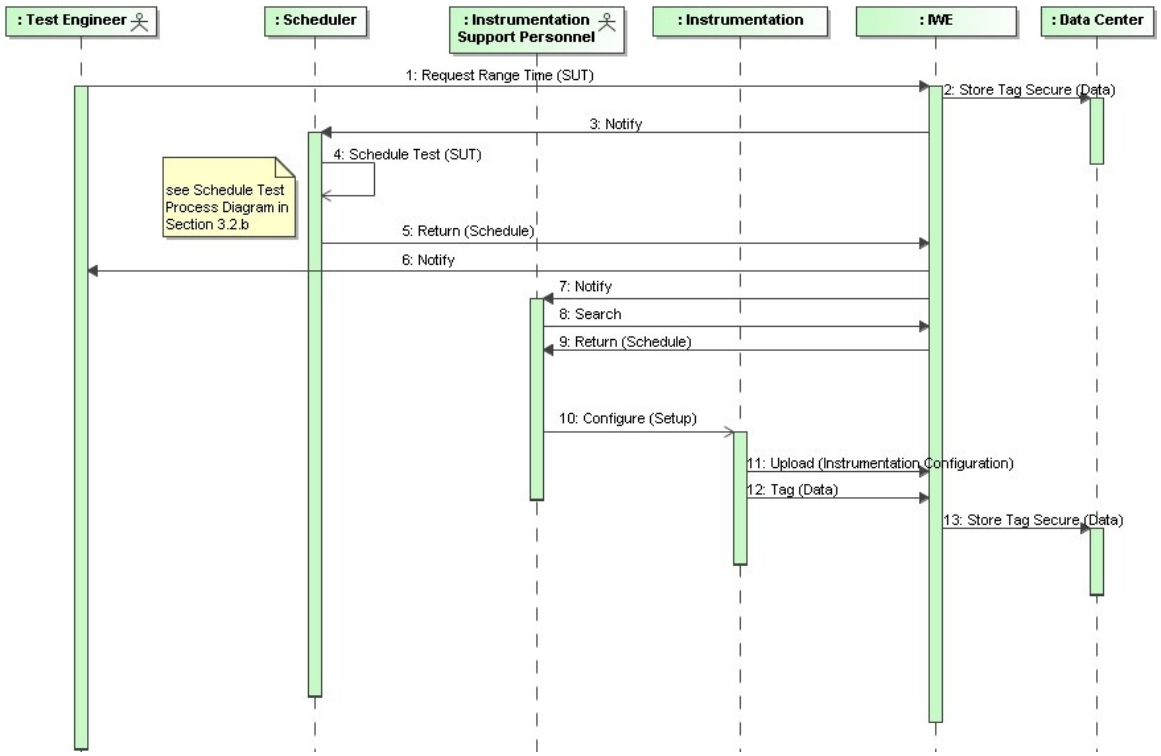

Figure 39. Pretest Setup Collaborations

b. Schedule Test Process in the Cloud

The process and collaborations for adding an event to the schedule and for event deconfliction would not change from the current process. However, having the schedule information accessible through the cloud would allow for rapid development of

new capabilities for the PM and all test personnel. One such function would be the ability for a PM to rapidly answer data calls, address scheduling conflicts and slippages, and so on.

For instance, if a program has multiple phases that cross TCs then this capability would give the PM visibility into TC Alpha, Beta, Charlie, and Delta's schedules. Within the IWE, the PM could establish true dependencies between the test milestones, regardless of what TC the testing will occur at. The test personnel would also benefit from the additional visibility into predecessor's schedules that the IWE would provide. If Alpha's schedule slips and Beta's start date is dependent on Alpha's test completing, then the POC at Beta could be automatically notified that Alpha has slipped, so Beta could adjust their schedule as necessary.

3. Test Execution Process in the Cloud

The test execution process is essentially the same in the cloud with the only changes being where the data is stored (Figure 40).

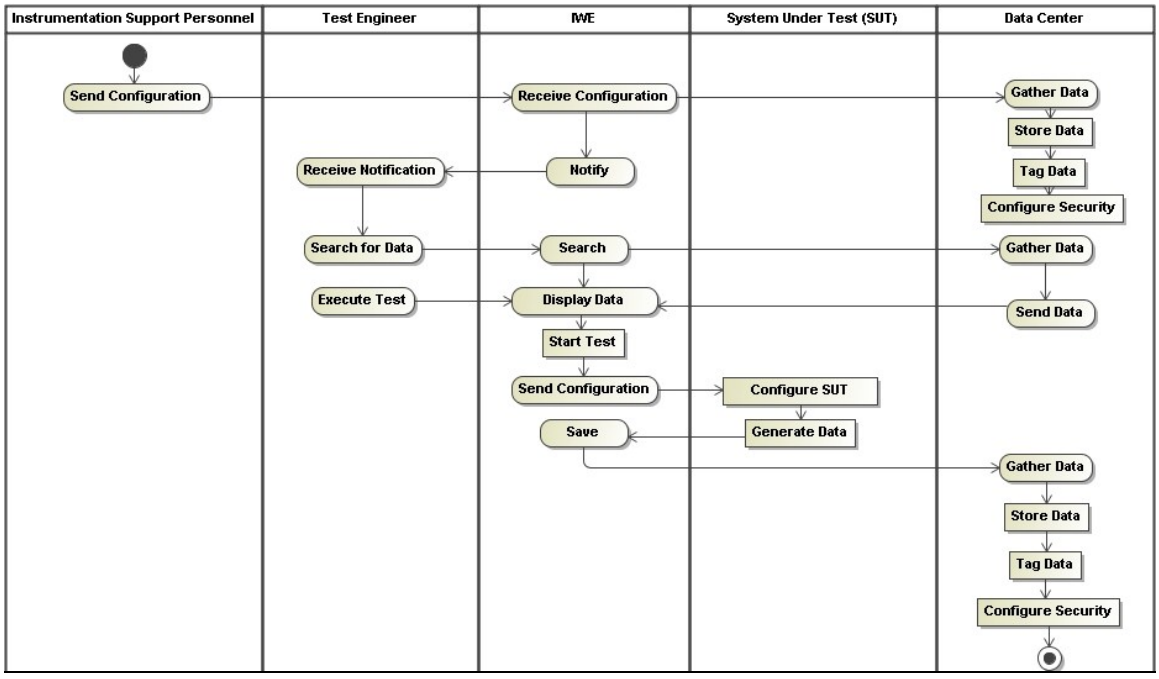

Figure 40. Test Execution Process in the Cloud

The cloud-enabled collaborations involved in the test execution process are also similar to the existing one. However, with the cloud approach, access control can be enforced in a uniform manner by the cloud services across the enterprise (Figure 41). Where the data is saved and how the security is set will be expanded on more in the following sections.

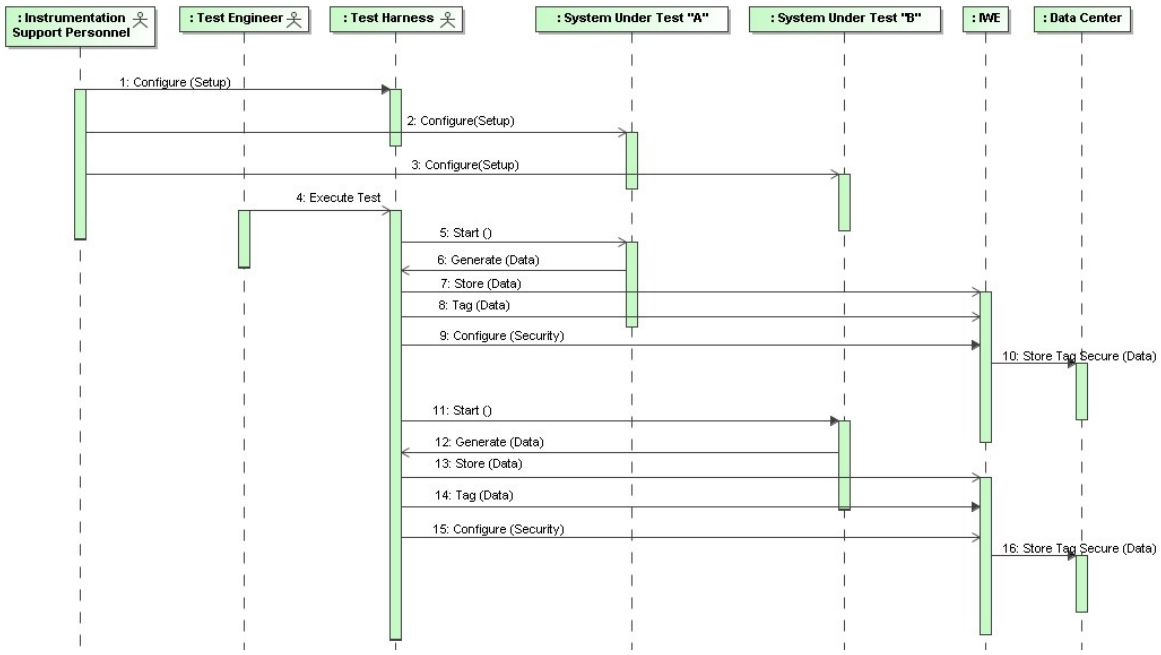

Figure 41. Test Execution Collaborations in the Cloud

4. Post-test Data Analysis Process in the Cloud

For a cloud environment to be a viable candidate for storing and processing T&E level 1 data (Table 10), it must have sufficient storage capacity, support efficient search relying on standard or custom tagging (similar to G-mail™), enforce access controls, support legacy data-reduction tools, save the reduced data back to the cloud with possibly new tagging, and provide non-reputable audit trails of access to the data and applications. The cloud must allow for the storage of structured and unstructured data, with and without associated metadata, and allow users to associate custom tags to data.

Data Level	Description	Possible Sources	Examples of Content	Disposition
Level 1 "raw data"	Data in their original form. Results of field trials just as recorded.	Complete data collection sheets, exposed camera film, voice recording tapes, original instrumentation magnetic tape or printouts, original videotapes, filled questionnaires, interview notes	1. All reported target presentations and detection 2. Clock times of all events 3. Azimuth and vertical angle from each flash base for each flash 4. Recording tapes of interviews	Accumulated during trials for processing. Usually discarded after use. Not published
Level 2 "reduced data"	Data taken from the raw form and consolidated. Invalid or unnecessary data points identified as such with supporting rationale.	Confirmed and corrected data collection sheets, film with extraneous footage identified corrected tapes or printouts, and original raw data with "No test" events identified.	1. Record of all valid detections. 2. Start and stop times of all applicable events. 3. Computed impact points off each round flashed. 4. Confirmed interview records.	Produced during processing. Usually files after use. Not published
Level 3 "ordered data"	Data that have been checked for accuracy and arranged in convenient order for handling. Operations limited to counting and elementary arithmetic.	Spreadsheet, tables, typed lists, ordered and labeled printouts, purified and ordered tape, edited film, edited magnetic tapes.	1. Counts of detections arranged in sets showing conditions under which detections occurred. 2. Elapsed times by type of event. 3. Impact points of rounds by condition under which fired. 4. Interview comments categorized by type.	Not usually published but made available to analysts. Usually stored in institutional data banks. All or part may be published as supplements to the test report
Level 4 "findings" or summary statistics	Data that have been summarized by elementary mathematical operations. Operations limited to descriptive summaries without judgments or inferences. Does not go beyond what was observed in the test.	Tables or graphs showing totals, means, medians, modes, maximums, minimums, quartiles, deciles, percentiles, curves, or standard deviations. Qualitative data in form of lists, histographs, counts by type, or summary statements.	1. Percentage of presentations detected. 2. Mean elapsed times. 3. Calculated probable errors about the centers of impact. 4. Bar graph showing relative frequency of each category of comment.	Published as the basic factual findings of the test.
Level 5 "analysis" or	Data resulting from statistical tests of	Results of primary statistical techniques such as T-tests, Chi-	1. Inferred probability of detection with its confidence interval.	Published in evaluation reports.

inferential statistics	hypothesis or interval estimation. Execution of planned analysis data Includes both comparisons and statistical significance level. Judgments limited to analyst's selection of techniques and significant levels.	square, F-test, analysis of variance, regression analysis, contingency table analyses and other associated confidence levels. Follow-on tests of hypotheses arising from results of earlier analysis, or fallback to alternate non-parametric technique when distribution of data does not support assumption of normality. Qualitative data in the form of prevailing consensus.	2. Significance of difference between two mean elapsed times. 3. Significance of difference between observed probable error and criterion threshold. 4. Magnitude of difference between categories of comments.	(If evaluation report is part of test report, the level 5 analysis results are presented separately from the level 4 findings.)
Level 6 "extended analysis" or operations	Data resulting from further analytic treatment going beyond primary statistical analysis, combination of analytic results from different sources, or exercise of simulation or models. Judgments limited to analysts' choices only.	Insertion of test data into a computational model or a combat simulation, aggregation of data from different sources observing required disciplines, curve fitting and other analytic generalization, or other operations research techniques such as application of queuing theory, inventory theory, cost analysis, or decision analysis techniques.	1. Computation of probability of hit based on target detection data from test combined with separate data or probability of hit given detection. 2. Exercise of attrition model using empirical test times distribution. 3. Determination of whether a trend can be identified from correlation of flash base accuracy data under stated conditions from different sources. 4. Delphi technique treatment of consensus of interview comments.	Published as appropriate in evaluation reports.
Level 7 "conclusion" or evaluation	Data conclusions resulting from applying evaluative military judgments to analytic results.	Stated conclusions as to issues, position statements, challenges to validity or analysis.	1. Conclusion as to whether probability of detection is adequate. 2. Conclusion as to timeliness of system performance. 3. Conclusion as to military value of flash base accuracy. 4. Conclusion as to main problems identified by interviewees.	Published as the basic evaluative conclusions of evaluation reports.

Table 10. Levels of Data from (ATEC, 2004)

Removing the data processing from the local desktop and placing it in a scalable cloud environment would address the data reduction performance requirements, provided the bandwidth between the user and the reduction tools is adequate. This could reduce the amount of time required for data reduction while also providing additional capabilities for users. Moving the data and tools to the cloud could also help eliminate or at least minimize the number of copies of data that are currently stored.

In a cloud solution, there would be minor changes in the Post-test Data Reduction process. Such as the location where the data is saved post test, where the reduction tools reside, and the location where the TE performs the reduction. Rather than the ISP storing the collected data on a local range server it could be stored in a cloud data center.

Going back to the scenario described in Chapter III, the ISP know which scheduled test the data is being collected for. So, with the creation of an IWE interface, the scheduling meta-data could automatically be associated with all data uploaded to the data center by the ISP by selecting from a list of test events that were completed at their range on a certain date. At the time of upload, the ISP could also tag the uploaded data with custom metadata that they think is pertinent. The metadata will provide a mechanism for the indexing and searching of the raw data at a later date.

When the metadata from the schedule is pulled into the system, the initial permissions could also be established to restrict access to only the POC that was listed in the schedule tool, who is likely the TE (Figure 42). That TE could then access the IWE from any approved computing device with network connectivity to the cloud, viewing the latest data uploaded by the ISP.

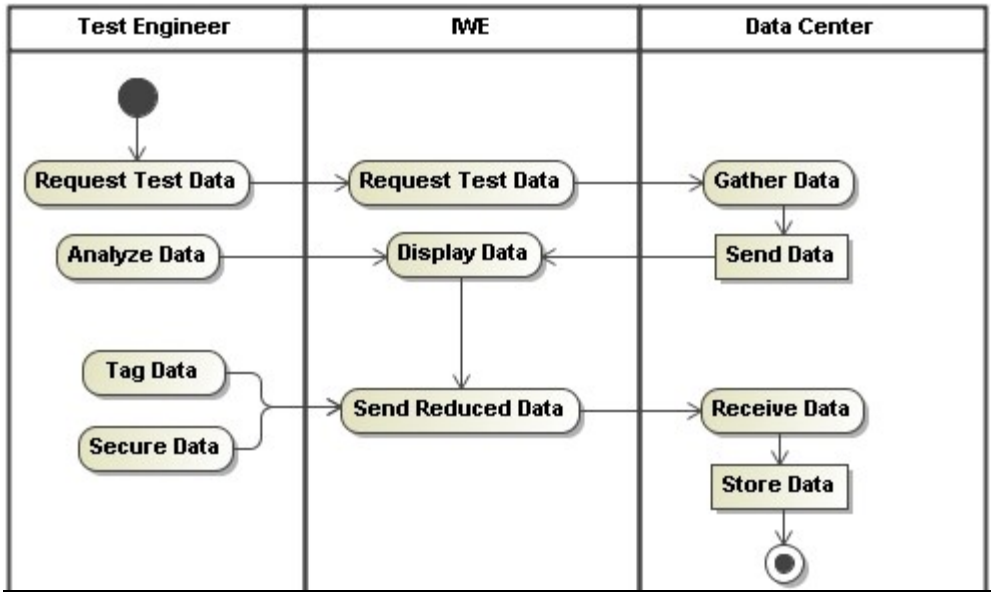

Figure 42. Post-test Data Analysis Process in the Cloud

The TE would have the ability to set permissions on the data, add additional custom tags, or begin the process of analysis and reduction (Figure 43) using tools based in the cloud. During analysis and reduction, the TE and needed tools would merely reference the data located in the cloud data center rather than the local range server.

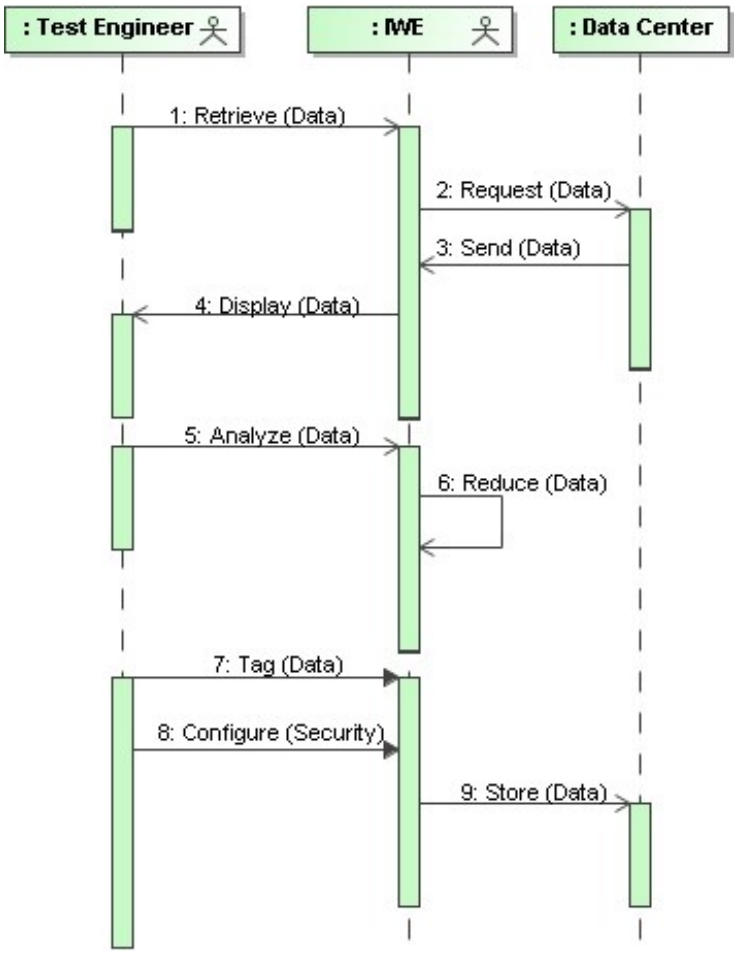

Figure 43. Post-text Data Analysis Collaborations in the Cloud

Duplicate data reduction could be obtained through reduction of logical copies, however, not physical copies. There is an important but subtle difference between the two. Physical copies are made by organizations for either fault tolerance or performance reasons and the enterprise system knows how to handle these files (e.g., file backup from June 1, 2010). A logical copy refers to copies of the same file or information at multiple locations that are not related, which the enterprise knows nothing about, only the user knows that they are related. For example, while reducing level 1 data a TE may end up with four copies of a single file: one on the TC enterprise shared projects server location (for sharing with others), one on a notebook hard drive (for access while TDY), one on a desktop hard drive (for heavy processing while in the office), and one on a private storage

location on the server (user's manual file versioning/backup solution) (Foster et al., 2010a). The relationship between all of these versions is only known to the TE.

To make the matter worse, any of the logical copies that are stored on an enterprise server also have physical copies. By moving the data and reduction tools into the cloud, four logical copies for one user have just been turned into one copy. Having a single copy of the data would also reduce the configuration management and control issues that arise from multiple users working on the same document and creating multiple logical copies. Moving the data to the cloud also provides users the option to access the data through the IWE from anywhere and via any authorized device. This capability could eliminate the need for logical copies on both the desktop and notebook hard drives.

a. Test Report Generation Process in the Cloud

The test report generation process within the cloud (Figure 44) would be much simpler than the current process with all actors being abstracted into three generic roles: Author, Reviewer, and Customer. In the current process multiple actors fill the role of Author and Reviewer depending on where they were in the process. For example, the TE and TM are both authors, the TE of the draft TE TR and the TM for the compilation of the final TR, and since the TE delivers its report to the TM then the TM can also be considered a customer.

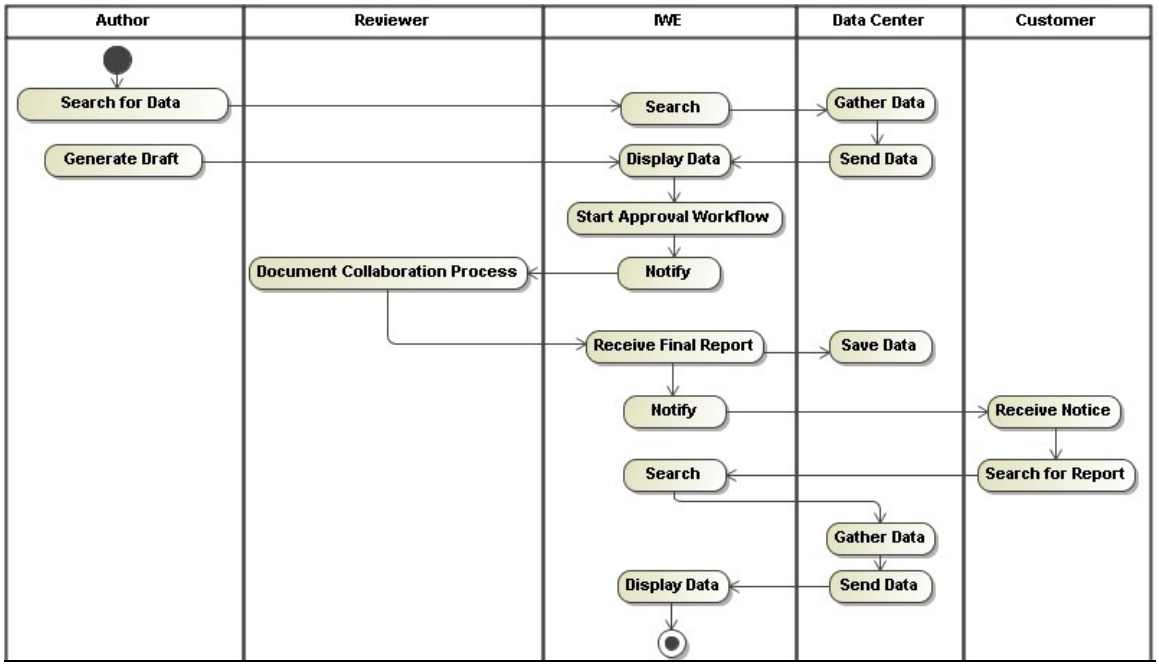

Figure 44. Test Report Generation Process in the Cloud

The test report generation collaborations in the cloud process would revolve around the IWE (Figure 45). Since everything would be accessible from within the IWE, all actors would be able to perform their collaborations within the same environment. The passing of artifacts back and forth through e-mail, uploading/downloading of TRs to/from a middleman storage area, and the manual e-mail notifications would be gone. The manual notifications could be replaced with a message board, wiki, etc. within the IWE or simply with automated notifications. More detailed information about the collaborations within the IWE is provided in the next section.

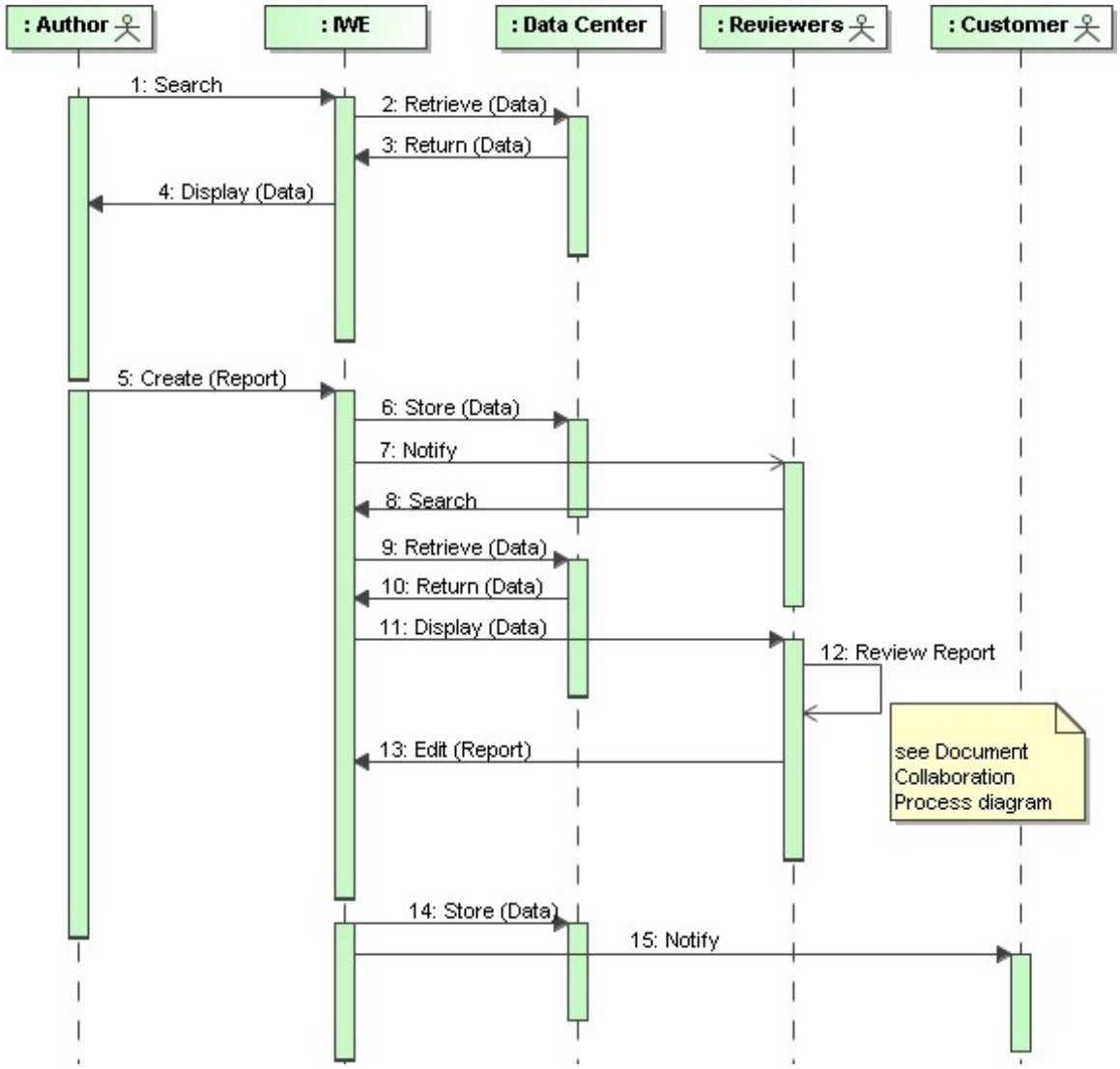

Figure 45. Test Report Generation Collaborations in the Cloud

In addition to streamlining the current process, having all of the TR information within the cloud would provide new capabilities. Having the various TR workflows accessible by the IWE, combined with the previously mentioned scheduling information would provide a new capability for all actors. The new capability would allow all actors post test to track where the TR is at in the generation process.

Having this information readily available would make it easier to establish standard metrics for time taken from the end of a test event through the delivery of a final TR. This information could be visible to all involved actors (TE, Supervisor, TD, TM,

and PM) with everyone able to see how long the TR stays in a particular location before moving on to the next reviewer or contributor. In other words, anyone with the proper access rights could view where the TR is at in the overall process, and ultimately, any bottlenecks in the process would be readily identified and resolved. As authors and reviewers made updates to the TR, they could add notes or tags into the status to indicate potential delays. That information could then be rolled-up into an overall status for the PM, who in turn could drill down to see that, for example, the TE report at TC Alpha is delayed at functional Division Delta while the TC Beta final TR is in the final steps of review.

These TR delivery metrics could be one tool available for senior leadership to use in determining if moving to a cloud-based environment increased efficiency. Through the compilation of an average TR delivery time from the completion of a test until delivery of the final TR, over many different programs, for a period of time before and after a move to a cloud environment senior leadership would have a good representation of the effect of moving to a cloud.

5. Document Collaboration Process in the Cloud

Currently, most of the interactions for reviewing and collaborating on documents occur through e-mail. This process could be greatly improved through the usage of social networking tools accessed through the IWE. Doing so would allow anyone with access to quickly see what has occurred recently with the program. So, if a TE goes TDY during the middle of collaborating on the final TR, then while on TDY, the TE could view what activities were occurring, what communications were ongoing between the various editors, status of scheduling, and continue to stay aware of the current situation all while on TDY.

If an online document editor were utilized for the creation and editing of the TR, then the TE could continue to collaborate and work on the document regardless of where the TE was physically located. The author, contributors, reviewers, and customer would all be users of the same online document editing tool. However, each would have

different permissions and would be participants at different stages in an overarching workflow. A change in status of some arbitrary metadata (such as changing from draft to final) could signal the document editing tool to start a workflow. The workflow could send notification to the reviewers that the document is ready for review.

This notification could be sent by various means such as e-mail, tweet, hot topic posting, RSS feed, etc. The reviewers would then go to the IWE, review the document, and either approve the document, which would change the metadata from draft to final resulting in the next workflow participant being notified. Or the reviewer could suggest changes to the document by adding comments either into the document or into a message board within the program workspace. The contributor that started the review workflow step would then be notified and the process would start over (Figure 46).

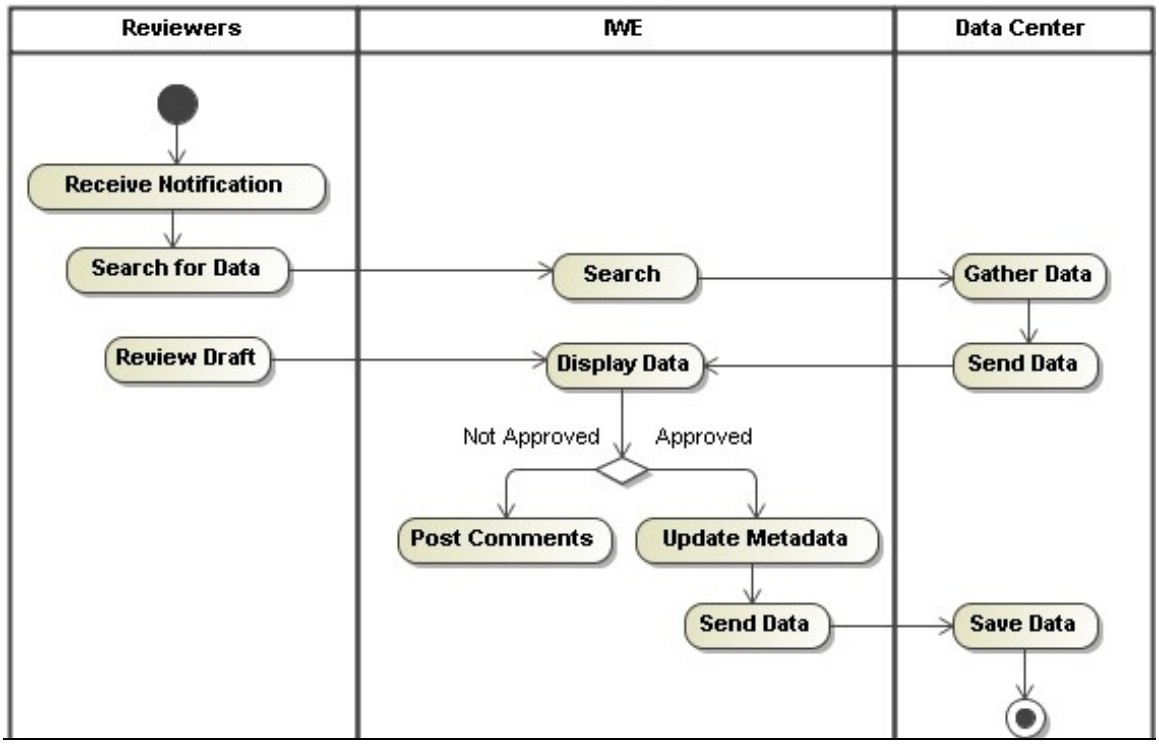

Figure 46. Document Collaboration Process in the Cloud

C. USE CASE ANALYSIS SUMMARY

The Use Case diagram, shown below (Figure 47), is unchanged from Chapter III and is displayed only for the convenience of the reader. Just as in Chapter III, the model is made up of nine use cases, described in Tables 11–19, with the differences between the Chapter III scenarios and the cloud computing scenarios being shown in italic. A table is also provided to summarize all T&E processes which would be modified in a move to a cloud-based environment.

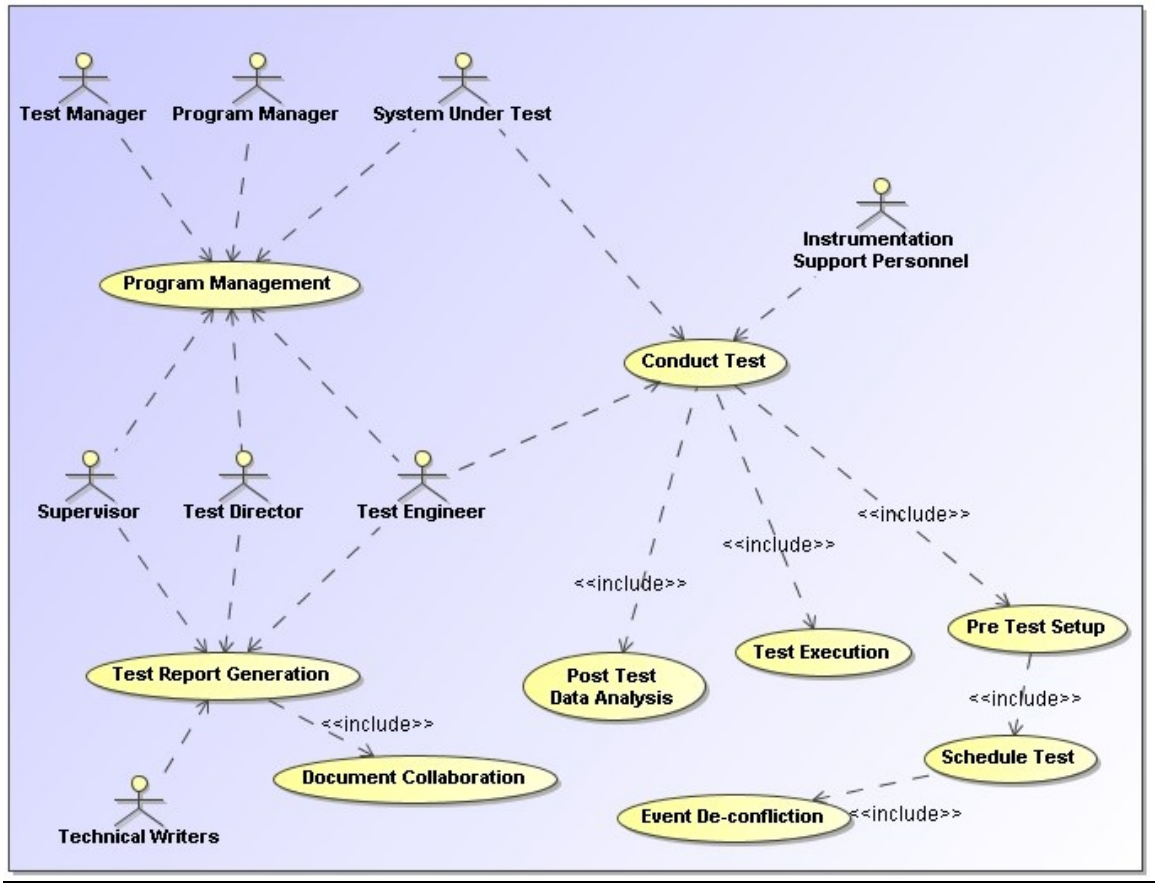

Figure 47. Cloud Mission Thread Scenario

UC10	Program Management	
Description	A Program Manager (PM) requests a new LFT&E test.	
Desired outcome	A test program is initiated with the test requirements flowing from the PM to the appropriate TC and eventually to the appropriate TE for the test.	
Assumptions	None	
Actors	• Program Manager (PM) • Supervisor • System Under Test (SUT) • Test Center (TC) • Test Director (TD) • Test Engineer (TE) • Test Manager (TM)	
Dependencies	None	
Process flow	Step description	Artifact
	1. PM submits a Request for Test Services (RFTS) to the IWE	*RFTS created*
	2. PM Inputs requirements into IWE	*Program Shell created* *ADSS Effort Shell created*
	3. TM Notified	
	4. TM Reviews Requirements	
	5. TM selects Test Center (TC)	*IWE TC Updated*
	6. TM activates Effort	Effort activated within ADSS
	7. TC Notified	
	8. TC Reviews Requirements	
	9. TC selects TD	*IWE POC updated* ADSS TC POC field updated
	10. TD Notified	
	11. TD reviews requirements	
	12. TD generates Test Plan	Initial Test Plan created ADSS Milestones updated

		VDLS Folder Structure created *Metadata*
	13. TD selects Division	*Metadata*
	14. Division Supervisor notified	
	15. Division Supervisor reviews requirements	
	16. Division Supervisor selects TE	*Metadata*
	17. TE Notified	
	18. TE Reviews test plan	
	19. TE performs test	
Deliverables	• ADSS Effort • Initial Test Plan • Project Plan • Test Requirements	
Additional information	None	

Table 11. Use Case 10: Program Management

UC11	Conduct Test
Description	Using the requirements and initial test plan a test will be conducted. This will require pretest planning, scheduling coordination, event deconfliction, test execution, and post test data analysis.
Desired outcome	To successfully conduct the test, obtain the data elements that will allow the TE to properly evaluate the SUT, and reduce the data in preparation for the generation of a formal Test Report.
Assumptions	• Funding has arrived, safety fans have been created, and environmental impact concerns have been addressed. • No external issues exist to prevent test from occurring. • System Under Test (SUT) is onsite at the Test Center (TC)
Actors	• Instrumentation Support Personnel (ISP) • Test Engineer (TE) • System Under Test (SUT)

Use cases involved	• Post-text Data Analysis UC16 • Pretest Setup UC12 • Test Execution UC15	
Dependencies	• Initial Test Plan • Test Requirements	
Process flow	Step description	Artifact
	1. Pretest setup	Finalized test plan
	2. Schedule test	Test on authoritative schedule
	3. Test execution	Raw test data collected
	4. Post test data analysis	Test data reduced
Deliverables	• Finalized Test Plan • Scheduled Test • Raw Test Data • Reduced Test Data	
Additional information	None	

Table 12. Use Case 11: Conduct Test

UC12	Pretest Setup
Description	Prior to test execution a great deal of upfront planning must occur. The test plan must be finalized, instrumentation must be configured, schedules must be coordinated, the test must be added to the authoritative schedule, and test setup information must be fully documented.
Desired outcome	To perform the proper upfront planning and coordination for the test execution to be repeatable and be executed with as few oversights as possible.
Assumptions	• Test Plan has been finalized.
Actors	• Instrumentation Support Personnel (ISP) • Schedule Test Process • Scheduler • Test Engineer (TE)

Use cases involved	• Schedule Test Process UC13	
Dependencies	• Initial Test Plan • Test Requirements	
Process flow	Step description	Artifact
	1. Test Engineer requests range time*	Schedule Request
	2. Test scheduled by Schedule Test Process* (UC13)	Authoritative Schedule for SUT
	3. Notify ISP and TE	
	4. ISP configures instrumentation	Instrumentation Configuration Plan
	5. Upload Configuration Plan to IWE	
	6. Tag, secure, and store data	*Configuration Plan Meta Data*
Deliverables	• Schedule Request • Instrumentation Configuration Plan • Authoritative Schedule for SUT	
Additional information	* Step 1 and 2 will continue will continue until the requested schedule successfully goes through the Schedule Test Process (UC13).	

Table 13. Use Case 12: Pretest Setup

UC13	Schedule Test
Description	Put a test on the authoritative range schedule.
Desired outcome	Successfully schedule range time and all required resources needed to support a test.
Assumptions	• All required resources are known and identified prior to scheduling test
Actors	• Event De-confliction Process • Scheduler • Test Engineer
Use cases involved	• Event De-confliction (UC14)

Dependencies	• Final Test Plan	
Process flow	Step description	Artifact
	1. * Schedule Request received from Test Engineer	Proposed Request
	2. * Conflicts identified by Event De-confliction process (UC14)	
	3. Conflicts resolved	Test Engineer notified Test added to Authoritative Schedule
Deliverables	• Authoritative Schedule for SUT	
Additional information	* Step 1 and 2 will continue will continue until all conflicts are addressed.	

Table 14. Use Case 13: Schedule Test

UC14	Event De-confliction	
Description	Identify and resolve potential scheduling conflicts prior to test events being added to the authoritative schedule.	
Desired outcome	To have a fully deconflicted schedule, so there is not a schedule delay due to lack of prior coordination between test programs.	
Assumptions	None	
Actors	• Authoritative Schedule Information • Conflictor • Conflictor Data • Scheduler • Test Engineer	
Use cases involved	• Schedule Test (UC13)	
Dependencies	• Proposed schedule	
Process flow	Step description	Artifact
	1. Receive proposed schedule	
	2. Request scheduled events	
	3. Identify conflicts	List of conflicts

	4. Send conflict list to user	User Notified
Deliverables	• List of conflicts	
Additional information	If no conflicts are present then the user is notified that no conflicts were found. This process will repeat with UC13 until all conflicts are addressed.	

Table 15. Use Case 14: Event De-confliction

UC15	Test Execution	
Description	LFT&E test occurs and data is collected.	
Desired outcome	The test plan is executed with no problems with data being successfully collected, stored, tagged, and secured for later reduction by the Test Engineer (TE).	
Assumptions	• All conflicts have been handled and any manual resolutions have occurred. • All instrumentation has been configured properly • Competing contractors are not present	
Actors	• Instrumentation Support Personnel (ISP) • *Data Center* • *Integrated Working Environment (IWE)* • System Under Test (SUT) • Test Engineer (TE)	
Use cases involved	None	
Dependencies	• Test is on authoritative schedule • *Instrumentation Configuration Plan is complete and available on IWE* • *Final Test Plan is complete and available on IWE*	
Process flow	Step description	Artifact
	1. Instrumentation is configured	
	2. Test is executed	*Raw Data is generated*
	3. Raw data is collected and	*POC for test event in Schedule*

	uploaded to the IWE	*Tool is notified of location*
	4. *Data is tagged and secured*	*Metadata* *Secured Raw Data*
Deliverables	• Raw Test Data	
Additional information	None	

Table 16. Use Case 15: Test Execution

UC16	Post-test Data Analysis	
Description	Raw data is reduced by the Test Engineer (TE) into a useable form.	
Desired outcome	While reducing the raw data the TE begins evaluation of the System Under Test (SUT) and has enough information to generate a formal Test Report (TR).	
Assumptions	None	
Actors	• *Data Center* • Test Engineer (TE) • *Integrated Working Environment (IWE)*	
Use cases involved	None	
Dependencies	• Raw Test Data	
Process flow	Step description	Artifact
	1. *Search for data*	
	2. *Retrieve raw data*	
	3. *Analyze raw data*	*Reduced Data*
	4. *Tag, Secure reduced data*	*Metadata* *Secured Reduced Data*
Deliverables	• Reduced test data	
Additional information	None	

Table 17. Use Case 16: Post-test Data Analysis

UC17	Test Report Generation	
Description	Compilation of a Final Test Report based on the Test Engineer's analysis of the reduced data.	
Desired outcome	A fully documented Final Test Report that is delivered to the Program Manager and is used by senior leadership to evaluate the effectiveness of the System Under Test (SUT).	
Assumptions	None	
Actors	• *Author* • *Customer* • *Integrated Working Environment (IWE)* • *Data Center* • *Reviewer*	
Use cases involved	• Document Collaboration (UC18)	
Dependencies	• Reduced Test Data	
Process flow	Step description	Artifact
	1. *Search for reduced test data*	
	2. *Create Draft Test Report*	*Draft Test Report*
	3. *Tag, Secure Draft*	*Metadata* *Secured Draft*
	4. *Begin Draft Approval Workflow (UC18)*	
	5. *Notify Reviewers*	
	6. *Search for Draft Test Report*	
	7. *Review*	*Final Test Report*
	8. *Tag, Secure Final Test Report*	*Metadata* *Secured Final Test Report*
	9. *Notify Program Manager*	

Deliverables	• Draft Test Report • Final Test Report
Additional information	None

Table 18. Use Case 17: Test Report Generation

UC18	Document Collaboration	
Description	Transformation of the draft Test Report into a Final Test Report through an approval workflow with all pertinent parties.	
Desired outcome	To have an approved Final Test Report that all pertinent parties have been able to review prior to release.	
Assumptions	None	
Actors	• Contributors • Reviewers • *Integrated Working Environment (IWE)*	
Use cases involved	None	
Dependencies	• Draft Test Report	
Process flow	Step description	Artifact
	1. * *Notification sent to Reviewers*	
	2. * *Search for Draft Test Report*	
	3. * *Review Draft Report*	*Comments*
	4. *Approve Draft Report*	*Final Test Report*
	5. *Tag Report*	*Metadata*
Deliverables	• Final Test Report	
Additional information	• Steps 1, 2, and 3 are continued until all comments are addressed and all reviewers approve the draft.	

Table 19. Use Case 18: Document Collaboration

Capability	Description of Change due to Cloud Environment
Program management	Semi-automated cloud-based communications/collaborations within the IWE could replace the current manual serial process for the monitoring, reporting, and controlling of a program.
Cloud-based data storage	Storing data locally impedes information sharing with ATEC and ATEC's stakeholders. Having all artifacts either stored in the cloud, or accessible from the IWE would expedite the sharing of data amongst all stakeholders, while also reducing the number of copies of data stored.
Accessible from anywhere	Artifacts within the IWE, to include communications and collaborations, could be viewed from any authorized network enabled device (e.g., computer, smartphone). Legacy data and applications could be accessed through the IWE until the data or application could be migrated to the cloud.
Collaboration	Using the IWE and the associated cloud-based collaboration as the primary mechanism for collaboration between all personnel involved in the T&E process would also help DoD amass the large amount of undocumented corporate knowledge employees currently posses, in their heads, into documented and searchable data.
Data tagging	IWE would allow for automatically tagging and securing of data based on available meta-data and will also allow users to add or associate custom tags to data as needed.
Data reduction	Data reduction tools could be hosted within the cloud and accessed through the IWE. Data reduction could occur within the IWE with reduced artifacts being saved back to the IWE with new tags.
Document collaboration	Document reviews could occur directly within the IWE, the document could start out within the IWE, go through all review processes within the IWE replacing the current method of passing artifacts back and forth through email and using middleman storage areas.
Security	All data accessed via the IWE would be protected through the use of RBACs and the IWE would provide non-reputable audit trails of access to the data and applications.
Situational Awareness	Schedule and financial information, as well as other

	information, could be viewed across all test centers and through a mash-up of data would provide a true situational awareness of the overall program.
TR delivery metrics	Standardized metrics could be created to measure the amount of time creating a TR requires from the end of testing until delivery to the customer, with authorized users able to view where the TR is within the process at any given time.
Search	The IWE should allow authorized users to search for and retrieve, security trimmed results, artifacts through user-friendly searches. Made possible through the indexing of all data regardless of whether the data is structure or unstructured and whether it has metadata or tagging associated or not.

Table 20. Summary of Changes for Cloud T&E Process

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND FUTURE RESEARCH

A. KEY FINDINGS AND RECOMMENDATIONS

In this thesis, we analyzed the existing workflow processes that Army T&E users follow during the execution of a T&E program. We then assessed how cloud computing can be used to streamline these workflows.

In the course of documenting the Army T&E workflow processes, we focused our attention on communications, and collaborations within the enterprise. This included communications starting with a request for test services, followed by scheduling a test and compilation and delivery of a final test report. The documentation consisted of scenarios, activity diagrams, and collaboration diagrams for nine use cases. During the analysis of the current system use cases, we determined that the current system relies heavily on e-mail as the primary means of communication and file transport. This can result in delays in the delivery of information to the PM as information is relayed from the PM down through the chain of command to the TE and then back up the chain of command to the PM. These delays can potentially affect decisions made by the PM and senior leadership.

The use cases, activity, and collaboration diagrams mentioned above were then reworked to show how the processes could be improved upon to leverage the communication and collaboration capabilities afforded by cloud computing. We determined that it is possible to streamline several of the current processes, which were based on manual or e-mail collaborations. Specifically the Program Management process, Test Report Generation process, and the Document Collaboration process would all benefit from a move to the cloud. These three processes and potential improvements are to some extent generalizable beyond the T&E domain. For instance the Document Collaboration process is applicable within every DoD environment that edits documents and the collaborations within the Program Management process would be applicable across multiple services, that is, beyond just the Army.

The streamlining could be realized through the use of cloud-based collaboration tools such as: online document editors, instant messaging, threaded message boards, wikis, blogs, tags, status updates, news, hot topics, tasks, and RSS feeds. These collaboration tools, along with all collected data associated with a program, would be accessible through an IWE. The IWE would provide a central location for storing, reducing, and collaborating on all information related to a program replacing e-mail as the primary means of collaboration and file transport. Where possible the IWE would interface with, and display information from, legacy ATEC Enterprise systems such as ADSS and SOFIMS.

The establishment of an IWE would greatly assist in the timely delivery of information to the PM and across the entire enterprise. The IWE would provide a mash-up of scheduling, financial, and other programmatic information that the PM, or anyone else with proper access rights, could access and pull information from on an as needed basis. Although the PM's workflow did not change substantially, by freeing the PM up from the timely manual tasks of collecting information about programs undergoing T&E, he or she can better use that freed up time. The effects of improving and modifying the PM's workflow process will be propagated to the related workflow processes of others, at a minimum the units of the enterprise that support the PM and ultimately the customers and other stakeholders.

Although this thesis focused solely on the Army T&E processes, it is likely that any improvements obtained by moving the Army processes to the cloud would also be applicable for Joint T&E programs. Joint system T&E programs, meaning systems that are utilized across multiple services such as the Ballistic Missile Defense System (BDMS), are faced with the same type of communications and collaborations as the Army processes. However, joint programs also have to manually maneuver through each service's unique T&E workflow process. The IWE could serve as an interface to the data and applications in the cloud, with the workflow details of the different services being transparent to the user.

We identified some specific ways in which to support the workflow of the PM such as enabling the PM to create a composite view of the schedule for the entire program, regardless of how many test centers are involved in the program. The advantage to the PM of having access to such a view of the data is that he or she can learn about slippage at one range that may affect another test center's long range schedule. At the other end of the spectrum, having all test data for a program stored, accessed, and processed through the IWE would allow the ISP to automatically secure the data based on the POC listed in the schedule tool. This would remove the burden from the TE while also reducing the risk of a competing contractor stumbling across a competitor's data.

The success or failure of the IWE concept will rely heavily on its ability of to provide Google-like search capabilities. Users should be able to search on both structured and unstructured data, without requiring the user posing the query to add metadata or tag the data. Within the scenarios of this thesis we assumed that the user would tag the data upon either initial collection or at any major milestone such as changing the status of a document from draft to a final release. This assumption may be unrealistic within a real-world setting in which the manual process is unreliable. If the tagging of the data cannot be automated in some fashion, such as by pulling the scheduling tool metadata in, then the crux of the IWE will always be limited by its search and index functionality.

B. CONCLUDING REMARKS

If the history of technology repeats itself, those prepared for IT change will be better positioned to take full advantage of new opportunities ("Cloud computing: Paradigm shift or just hype," 2008). Cloud computing is a disruptive technology whose implementation will require change across all levels of DoD. It will require technical training and a cultural shift in how DoD senior leadership, program management, end users, customers, suppliers, and especially IT professionals think about IT resources. This shift will require changes in all aspects of the acquisition of IT. In addition to the technical challenges, there will be challenges in aligning the corporate culture with the new workflows and associated means of communication and collaboration.

The cultural issues surrounding a user's trust that the network will be there when it is needed will be one of the most difficult challenges to overcome. In DoD, as at many organizations, if you own it, you control it (Zyskowski, 2010). As an IT professional, if you cannot go into a cold server room and see a row full of blinking lights, hear fans humming, and have the ability to 'hug the server' how can you trust that it will be there when your users and senior leadership requires it? As a senior leader, how do you overcome the fear associated with no longer having someone in your chain of command who you can 'reach out and touch' 24/7 if a business critical capability goes offline? In the current atmosphere, most critical servers and applications reside locally, and if a capability fails, fixing it is merely a matter of dedicating enough man hours and hardware to repair the system. In a public or private cloud environment, you are potentially placing cloud-services providers, outside of your immediate control, directly into your IT department's critical path for keeping systems available and operating correctly.

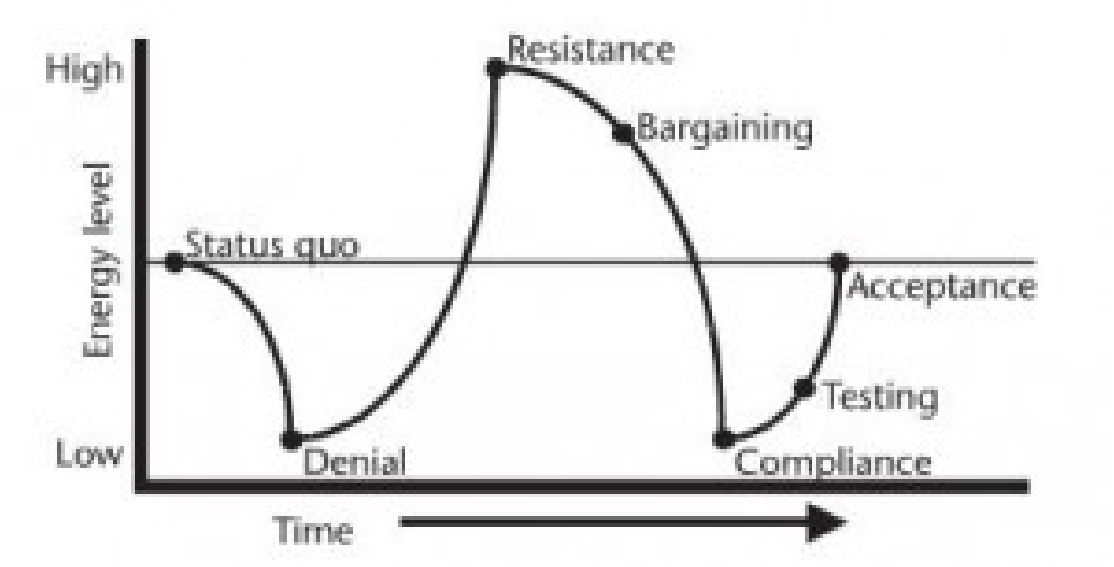

Figure 48. Response to change from (Koch, 2004)

While change is natural and good, the typical first reaction to change is resistance that comes from a fear of the unknown or an expectation of loss (Figure 48). Resistance

to cloud computing will be met, and for DoD's transformation to succeed, this resistance must be overcome. In general, fighting human nature is an uphill battle that eventually results in failure. However, by working to educate stakeholders on what cloud computing is, defining what will change, why it needs to change and getting a mutual understanding from key stakeholders, hopefully their resistance to change can be overcome.

C. FUTURE WORK

While cloud computing is still in its infancy, this research has shown that it does bear promise cut the cost of delivering IT services to the DoD community, other things being equal. However, there are lots of open research questions, some of which we mention below:

1. Near Term

a. Network Bandwidth Measurement

Network speed between the end user and the cloud will be a potential stumbling block. Many TCs are in remote locations and have limited network bandwidth. The fiber infrastructure into these TCs will likely need to be improved prior to a large-scale move to a cloud environment. The rise of the use of Voice Over IP (VOIP) telephones will also increase the amount of network traffic. This could have a negative impact to moving large amounts of data into the cloud or trying to use cloud-based data-reduction tools via the network. Additional investigations should focus on gathering technical metrics and measuring the bandwidth of networks between various DoD locations and the as yet to be announced DoD APC cloud locations. These studies should focus on measuring available bandwidth over short and long distances to identify potential communication bottlenecks.

b. Additional Use Cases

Further investigations should be conducted to document user requirements and use cases beyond those identified in this thesis. This research should be conducted

within both the NIPRNet and DREN, as these two environments have different missions and requirements. Research should also be conducted on the secure side (e.g., SIPRNet and SDREN environments).

c. IT Technologist's Role Within the Cloud

Research should begin to identify the delta of a typical IT Server/Network administrator's daily duties today versus after their assets are deployed into a cloud environment. Vendors and cloud proponents claim that moving to the cloud will lead to a fundamental shift in IT goals enabling IT professionals to spend less time and effort on the data center and help desk activities. This freed up time theoretically would allow IT professionals to spend more time working with end users on business innovation and improvement projects.

d. Pathfinders and Pilot Programs

Pathfinder experiments should be created to test out cloud computing within DoD's multiple environments (e.g., NIPRNet, SIPRNet, DREN, SDREN). The pathfinders would allow researchers to evaluate the speed, security, usability, SLAs, and other aspects of potential cloud-based solutions.

After successful pathfinder experiments, multiple pilot programs should be created at locations geographically close to DoD APC cloud locations, as well as remote locations. The pilot programs should focus on moving small organizations into the cloud. This will assist DoD in getting any kinks out of the process prior to widespread adoption. The geographically close pilot could be used to demonstrate what theoretically should be a best-case scenario from a performance standpoint, while the remote location pilot could be used to identify issues that are likely to arise during widespread adoption.

The pilot programs would also provide an opportunity to evaluate the change in IT staff's responsibilities and duties. The upcoming Army APC2 implementation would be a good opportunity for research to begin from the ground floor and collect the metrics needed for the studies suggested above.

e. Security Concerns

Storing all test data within the same repository, whether physical or logical, and accessing through a common interface will raise issues with classification through aggregation. Research should address, among other things, ways to mitigate information leakage and the establishment of redaction procedures.

Research should also begin to identify whether current architectures are adequate for building trusted clouds, or if new architectures are needed. Whether current OS and application security approaches will scale properly to a cloud computing environment, or if new approaches will need to be taken to provide a trusted OS—such as the efforts currently underway within NPS and as described in the DoD IAnewsletter article titled “Establishing Trust in Cloud Computing”. (Dinolt & Michael, 2010)

f. Social Networking Tools

Further research should occur around the usage of social networking tools within DoD. This thesis only briefly touched on the potential usage of social networking tools within T&E. Current social networking tools should be evaluated for their applicability to advancing the DoD mission.

2. Long Term

a. Data Tagging, Indexing, and Searching

Further research should occur in the realm of automated tagging of data. The success of the ICW is predicted to rely, in some degree, upon the automated tagging of all data artifacts with metadata and the ability to efficiently search and index structured and unstructured data.

b. Tactical Applicability

Connecting multiple information sources together in a meaningful way to provide commanders and warfighters with a more complete picture is critical to making better decisions. Information should be just as available at the edge of the battlefield, senior leaders at headquarters, and TEs at the T&E ranges. Research should also be

undertaken on assessing the applicability of cloud computing to the tactical environment. Use cases should also be gathered for applicability to the warfighter on, or near, the frontlines. Some of the current research efforts include: “Cloud Computing for Large-Scale Weapon Systems” (Foster et al., 2010b) and “The Cloud and its Implications to Naval Warfare” (Hurlburt, 2010).

LIST OF REFERENCES

Abbott, M. & Fisher, M. (2010). *The art of scalability: scalable web architecture, processes, and organizations for the modern enterprise*. Upper Saddle River, NJ: Addison-Wesley.

Army Contracting Command. (2010, July 15). *Army private cloud computing services final solicitation. Federal Business Opportunities*. Retrieved August 4, 2010, from https://www.fbo.gov/index?s=opportunity&mode=form&id=2ef1899dcdaf2d7dd8609833fe508e14&tab=core&_cview=1

Army Regulation 385-63 (2003, May 19). *Range Safety*. Retrieved August 25, 2010 from https://acc.dau.mil/CommunityBrowser.aspx?id=243487

ATEC. (2004, April 19). *System test and evaluation procedures*. Retrieved from http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBgQFjAA&url=https%3A%2F%2Facc.dau.mil%2FGetAttachment.aspx%3Fid%3D240738%26pname%3Dfile%26aid%3D38783%26lang%3Den-US&ei=lTVlTK3LN4PGlQexsZ2TDg&usg=AFQjCNFVHJx5DHU57baSRR7li9gWVAljFA

Authers, J. & Mackenzie, M. (2010, March 9). *Techs reflect on decade since dotcom boom*. *Financial Times*. Retrieved May 26, 2010, from http://www.ft.com/cms/s/d66e80b6-2b95-11df-a5c7-00144feabdc0,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2Fd66e80b6-2b95-11df-a5c7-00144feabdc0.html&_i_referer=

Avoyan, H. (2010, April 27). *Cloud SLAs require extra attention*. *Cloud Computing Journal*. Retrieved July 3, 2010, from http://cloudcomputing.sys-con.com/node/1370805

Brodkin, J. (2009, April 30). *With long history of virtualization behind it, IBM looks to the future*. Network World. Retrieved August 24, 2010, from http://www.networkworld.com/news/2009/043009-ibm-virtualization.html

Bureau of Labor Statistics: *Career guide to industries*. (2010). *United States Department of Labor*. Retrieved July 2, 2010, from http://www.bls.gov/oco/cg/cgs041.htm

Carr, N. (2009). *The big switch: Rewiring the world, from Edison to Google*. New York: W.W. Norton & Co.

Carter, J. & Rajamani, K. (2010, July). *Designing energy-efficient servers and data* centers. IEEE Computer Society, 43(7), 76–78.

Chabrow, E. (2010, March 29). *FedRAMP could speed cloud adoption*. *Gov Info Security*. Retrieved June 23, 2010, from http://www.govinfosecurity.com/articles.php?art_id=2350

Christiansen, C., Hudson, S., Kolodgy, C., & Pintal, G. (2010, May). *Identity and access management for approaching clouds*. *IDC CA Technologies*. Retrieved July 11, 2010, from http://www.ca.com/files/IndustryAnalystReports/cloud_security_wp_236234.pdf

Clarke, G. (2010, June 25). *Chipzilla: Standards void threatens cloud future*. *The Register*. Retrieved June 25, 2010, from http://www.theregister.co.uk/2010/06/25/intel_microsoft_oracle_cloud_standards/

Cloud computing: Paradigm shift or just hype. (2008). *IBM*. Retrieved June 30, 2010, from https://www-304.ibm.com/businesscenter/cpe/html0/158782.html

Cloud Computing Use Cases White Paper v3.0. (2010, February 2). *Google Groups: Cloud Computing Use Case Discussion Group*. Retrieved June 28, 2010, from http://groups.google.com/group/cloud-computing-use-cases/files?pli=1

Cockburn, A. (2000). *Writing effective use cases*. Addison-Wesley.

Computer History. (2010). *plyojump*. Retrieved June 7, 2010, from http://www.plyojump.com/classes/hardware.html

Corrin, A. (2010, June 10). *Army steps up data center consolidation after imposing server moratorium*. *Government Computer News*. Retrieved June 11, 2010, from http://gcn.com/articles/2010/06/10/army-server-moratorium.aspx

Cueli, M. (2010, July 1). *The key concepts of cloud computing*. *PC World*. Retrieved July 6, 2010, from http://www.pcworld.com/article/200332/the_key_concepts_of_cloud_computing.html

Defense Acquisition Guidebook Ch. 9.7. Test and Evaluation reporting of results. (2010). *Defense Aquisition University*. Retrieved June 4, 2010, from https://acc.dau.mil/CommunityBrowser.aspx?id=315930

Defense Budget 2010. (2010). *Documents for small business and professionals*. Retrieved May 26, 2010, from http://www.docstoc.com/docs/5229722/Defense-Budget-2010

DoD Instruction 5000.02, Operation of the defense acquisition system. (2010). *Acquisition Community Connection*. Retrieved June 4, 2010, from https://acc.dau.mil/CommunityBrowser.aspx?id=44891

Dinolt, G. & Michael, J. (2010, Spring). *Establishing trust in cloud computing.* DoD IAnewsletter, Vol 13 No 2, pp. 4-8, Retrieved August 25, 2010, from http://iac.dtic.mil/iatac/download/Vol13_No2.pdf

DOE deploys cloud computing. (2010, February 22). *Information Technology Market*. Retrieved July 3, 2010, from http://www.informationtechnologymarket.com/?p=113

DiMaio, A. (2009, October 7). *Federal shift to cloud raises tough issues for CIOs*. *Government Technology*. Retrieved May 26, 2010, from http://www.govtech.com/gt/729707

Enterprise and SMB software survey North America and Europe. (2008, Q4). *Forrester Research, Inc.*. Retrieved June 7, 2010, from http://www.forrester.com/ER/Research/SurveyFile/0,5519,2024,00.pdf

Federal guidance needed to address control issues with implementing cloud computing. (2010, May). *Government Accountability Office*. Retrieved July 3, 2010, from http://www.gao.gov/new.items/d10513.pdf

Federal risk and authorization management program (FedRAMP). (2010). *Chief Information Officers Council*. Retrieved June 7, 2010, from http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP

Foster, K. D., Shea, J., Drusinsky, D., Michael, J., Otani, T., & Shing, M. (2010a, July). *Removing the boundaries: Steps toward a cloud nirvana*. Proceedings of the IEEE International Conference on Granular Computing, San Jose, California, 14-16 August 2010, pp. 167–171

Foster, K. D., Shea, J., Peitso, L., Michael, J., Otani, T., & Shing, M. (2010b, July). *Cloud computing for large-scale weapon systems*. Proceedings of the 2010 IEEE International Conference on Granular Computing, San Jose, California, 14-16 August 2010, pp. 161–166

Gallagher, S. (2010, April 7). *Army confronts battle to globalize its network resources*. *Defense Systems*. Retrieved June 11, 2010, from http://www.defensesystems.com/Articles/2010/04/06/Defense-IT-1-GNECs-Uphill-Climb.aspx

Gourley, B. (2009, March 21). *Cloud computing and cyber defense. Whitehouse*. Retrieved March 2, 2010, from http://www.whitehouse.gov/cyberreview/documents

Hoover, N. (2010a, April 14). Inside NASA's nebula compute cloud. *Information Week Government*. Retrieved June 29, 2010, from http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=224202583

Hoover, N. (2010b, July 30). *Army plans private cloud*. *Information Week Government*. Retrieved July 30, 2010, from http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=226300299&subSection=News

Hurlburt, G. (2010, July/Sept) *The cloud and its implications to naval warfare*, CHIPS, Retrieved August 24, 2010, from http://www.chips.navy.mil/archives/10_Jul/web_pages/cloud_computing.html

Jackson, K. (n.d.). *Cloud computing 101*. *XMind - Social Brainstorming and Mind Mapping*. Retrieved May 26, 2010, from http://www.xmind.net/share/_embed/kvjacksn/cloud-computing-101/

Jeffrey, NA. (2009, December 12). *Computing on cloud 9. Boomer Technophobia*. Retrieved June 7, 2010, from http://www.boomertechnophobia.com/cloud-computing

Johnson, C. (2003, June). *The Army Test and Evaluation Command*. *Army Logistics University*. Retrieved June 4, 2010, from http://www.almc.army.mil/alog/issues/MayJun03/MS865.htm

Kash, W. (2010, April 30). *FedRAMP: The dawn of approve-once, use-often? Government Computer News*. Retrieved June 7, 2010, from http://gcn.com/articles/2010/05/03/editorial-fedramp-long-overdue.aspx

Koch, A. (2004). *Agile software development evaluating the methods for your organization.* Artech House Publishers.

Kundra, V. (2010, May 20). *State of public sector cloud computing*. *Chief Information Officers Council*. Retrieved May 26, 2010, from http://www.cio.gov/pages.cfm/page/State-of-Public-Sector-Cloud-Computing

Leduc, M. (n.d.). *Timeline of the modern prime mover's development, the diesel engine and its development. Martin's Marine Engineering Page*. Retrieved June 7, 2010, from http://www.dieselduck.ca/library/04%20other/prime_movers.htm

Link, D. (2010, June 15). *Role of federal CIO, CTO influences agencies on cloud. Federal News Radio*. Retrieved June 22, 2010, from http://www.federalnewsradio.com/index.php?nid=249&sid=1980797

Lynn III, W.. (2009, November 12). *Remarks at the defense information technology acquisition summit. Department of Defense*. Retrieved May 26, 2010, from http://www.defense.gov/speeches/speech.aspx?speechid=1399

Malan, R, & Bredemeyer, D. (2001, August 3). *Functional requirements and use cases. Bredemeyer Consulting*. Retrieved August 11, 2010, from http://www.bredemeyer.com/pdf_files/functreq.pdf

Malan, R, & Bredemeyer, D. (2009, November 10). *The software architecting process. The Architecture Discipline*. Retrieved August 11, 2010, from http://www.bredemeyer.com/howto.htm

Management Steps Part 3. (2009, November 10). *Project management classroom*. Retrieved August 1, 2010, from http://projectmanagementclassroom.com/page/3/

Milburn, D. (2010, May 24). *Five SLA topics to address in selecting a cloud provider*. *Tech Journal South*. Retrieved July 3, 2010, from http://www.techjournalsouth.com/2010/05/five-sla-topics-to-address-in-selecting-a-cloud-provider/

Miller, J. (2009, December 10). *Agencies to justify not using cloud computing to OMB. Federal News Radio*. Retrieved June 29, 2010, from http://www.federalnewsradio.com/?sid=1836091&nid=35

Morton, G, & Alford, T. (2009). *The economics of cloud computing*. *Booz Allen*. Retrieved May 26, 2010, from http://www.boozallen.com/publications/article/42656904

Mullins, R. (2010, June 16). *IDC survey: Risk in the cloud. Network Computing*. Retrieved June 25, 2010, from http://www.networkcomputing.com/cloud-computing/cloud-minuses-outweigh-pluses-for-businesses.php?cid=NWC_report_2010-06-19_t

NASA flagship initiatives: Nebula. (2010). *NASA.Gov*. Retrieved June 29, 2010, from http://www.nasa.gov/open/plan/nebula.html

Nokes, S. (2008). *The definitive guide to project management: The fast track to getting the job done on time and on budget* (2nd ed.). FT Press.

Oltsik, J. (2010, May 5). *FedRAMP seeks to unify cloud computing security standards across the U.S. government. Network World*. Retrieved May 26, 2010, from http://www.networkworld.com/community/node/60847

O'Neill, M. (2009, April 27). *Connecting to the cloud, Part 1: Leverage the cloud in applications*. *IBM*. Retrieved May 26, 2010, from http://www.ibm.com/developerworks/webservices/library/x-cloudpt1/index.html

Orszag, P. (2009, June 11). *Planning for the President's fiscal year 2011 budget and performance plans*. *Whitehouse*. Retrieved May 26, 2010, from http://www.whitehouse.gov/omb/assets/memoranda_fy2009/m09-20.pdf

Price, D. (2007, February 14). *Stormy weather*. *LA Progressive*. Retrieved July 3, 2010, from http://www.laprogressive.com/the-environment/stormy-westher/

Prigge, M. (2010, June 21). *Cloud computing has jumped the shark*. *PCWorld Business Center*. Retrieved June 22, 2010, from http://www.pcworld.com/businesscenter/article/199438/cloud_computing_has_jumped_the_shark.html

Rapid Access Computing Environment (RACE). (2010). *Defense Information System Agency*. Retrieved May 26, 2010, from http://www.disa.mil/race/

Server consolidation and virtualization. (2010). *envirux clean it up*. Retrieved June 7, 2010, from http://www.envirnux.com/solutions/virtualization.asp

Sharma, M. (2008, June 16). *A virtual appliance primer*. Linux.com. Retrieved August 24, 2010, from http://www.linux.com/archive/feature/138166

Summary of NIST cloud computing standards development efforts. (2010). *National Institute of Standards and Technology*. Retrieved May 26, 2010, from http://csrc.nist.gov/groups/SNS/cloud-computing/

Tanenbaum, A. (2008) *Modern Operating Systems*, N.J.: Prentice Hall

Thompson, C. (2009, December 4). *A brief history of social network enterprise collaboration tools*. *VentureBeat*. Retrieved August 18, 2010, from http://venturebeat.com/2009/12/04/a-brief-history-of-social-network-enterprise-collaboration-tools/

U.S. Army Developmental Test Command. (2010). *US Army DTC Welcome*. Retrieved June 2, 2010, from http://www.dtc.army.mil/what.aspx

U.S. Army Evaluation Center. (2010). *US Army AEC About*. Retrieved June 4, 2010, from http://www.atec.army.mil/AEC/index.asp

U.S. Army Operational Test Command. (2010). *US Army OTC Mission*. Retrieved June 4, 2010, from http://www.otc.army.mil/mission.htm

U.S. Army Test and Evaluation Command. (2010). *US Army ATEC Mission/Vision*. Retrieved June 2, 2010, from http://www.atec.army.mil/mission_vision.htm

Warsh, D. (2006). *Knowledge and the wealth of nations: A story of economic discovery*. W. W. Norton.

West, D. (2010). *Saving money through cloud computing*. Retrieved from http://www.brookings.edu/~/media/Files/rc/papers/2010/0407_cloud_computing_west/0407_cloud_computing_west.pdf

What is use case? (2008, July 2). *Tech Terms*. Retrieved August 11, 2010, from http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci334062,00.html

Zyskowski, J. (2010, March 22). *Lt. Gen. Jeffrey Sorenson envisions a global Army network*. *Federal Computer Week*. Retrieved July 1, 2010, from http://fcw.com/articles/2010/03/22/feature-federal-100-sorenson-jeffrey.aspx

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Peter Denning
   Naval Postgraduate School
   Monterey, California

4. Professor Bret Michael
   Naval Postgraduate School
   Monterey, California

5. Professor Man-Tak Shing
   Naval Postgraduate School
   Monterey, California

6. Mr. John Shea
   Office of the DoD CIO
   Arlington, Virginia

7. COL Kevin Foster, USA
   Office of the DoD CIO
   Arlington, Virginia

8. Professor George Dinolt
   Naval Postgraduate School
   Monterey, California

9. Professor Doron Drusinsky
   Naval Postgraduate School
   Monterey, California

10. Professor Thomas Otani
    Naval Postgraduate School
    Monterey, California

11. Professor Loren Peitso
Naval Postgraduate School
Monterey, California

12. Mr. Alex Nelson
Naval Postgraduate School
Monterey, California

13. Mr. Scott J Dowell
Computer Science Corporation
San Diego, California

14. Mr. Michael Lee
Touchstone Consulting Group
Washington, D.C.

15. Ms. Karen Gordon
Institute for Defense Analyses
Alexandria, Virginia

16. Dr. Jeffrey Voas
National Institute of Standards and Technology
Gaithersburg, Maryland

17. Dr. Mark Lee Badger
National Institute of Standards and Technology
Gaithersburg, Maryland

18. Dr. Tim Grance
National Institute of Standards and Technology
Gaithersburg, Maryland

19. Mr. David Byrd
Redstone Test Center
Redstone Arsenal, Alabama

20. Mr. Charles Gibbs
Redstone Test Center
Redstone Arsenal, Alabama

21. Mr. Paul Jenkins
Redstone Test Center
Redstone Arsenal, Alabama

22. Mr. Tracy Mullendore
Dugway Proving Ground
Dugway, Utah

23. Mr. Brian Kessel
White Sands Missile Range
White Sands, New Mexico

24. Mr. Denis Gizinski
Yuma Proving Ground
Yuma, Arizona

25. Mr. Scott Redding
Aberdeen Proving Ground
Aberdeen, Maryland

26. Mr. John Graham
Developmental Test Command
Aberdeen, Maryland

27. Mr. Tom Clohan
Army Test and Evaluation Command
Alexandria, Virginia

28. Mr. David Browning
PEO Missiles and Space
Redstone Arsenal, Alabama

29. Mr. Ryan Norman
Test Resource Management Center
Arlington, Virginia